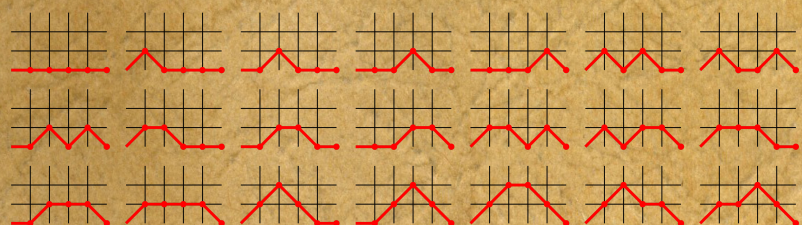
Notas
Incompletas de
Clase
Estudio 0

4.ª edición
enero de 2026

Cuestiones de MATEMÁTICAS DISCRETAS

Teoría y práctica

Volumen 0



Juan Miguel León Rojas

Revisión:
D:20260429201539+02'00'

Cuestiones de matemáticas discretas

Cuestiones de matemáticas discretas
Teoría y práctica
Volumen 0

Juan Miguel León Rojas

Apunte bibliográfico.— Una compilación a la vez que una republicación corregida y aumentada de materiales que, desde 2009, han ido viendo la luz, año tras año, como notas de clase, exámenes y sus soluciones.

Meta.— Formar una base sólida vía la práctica intensa.

En mejora continua. Si bien dejaron de ser un bosquejo, estas notas incompletas de clase (NIC) siguen siendo parte de un trabajo en curso. Algunas escuetas, abreviadas, otras detalladas, íntegras; todas continúan en el ciclo de revisión, corrección y actualización, intentando corresponder de alguna manera a la benevolencia y paciencia de todas las personas que han manejado o estudiado este material. Seguramente encontraremos errores —espero que la mayoría sean tipográficos—, si bien existe la posibilidad de que algunas áreas estén incompletas o incluso sean incorrectas (en esta edición, el índice de nombres y términos aún lo está y es). Perdonadme por esta vez, que fue sin malicia[-2].

Depósito legal.—

Ediciones.— ▪ 0.ª, septiembre de 2023; ▪ 1.ª, enero de 2024; ▪ 2.ª, enero de 2025; ▪ 3.ª, mayo de 2025; ▪ 4.ª, enero de 2026. La presente edición puede consultarse y descargarse libremente de https://archive.org/details/leon-rojas-j.-m.-2024-cuestiones-de-matematicas-discretas.-volumen-0. En concreto, la revisión de esta edición que tenemos en nuestras manos es la D:20260429201539+02'00'. Prestemos atención a dicha página web pues es donde aparecerá la edición o revisión última.

Imagen de portada.— *Una interpretación de los números de* Motzkin[○] —la imagen de fondo de la portada y contraportada es *Vintage Paper Texture (9789792113)*, de James Puckett, con licencia Creative Commons Attribution 2.0 Generic—[1].

Los ingredientes sustanciales de estas NIC son de origen matemático.
Compuestas y publicadas en España, siguen siendo empíricamente comprobadas.

[-2] Esta frase la tomo prestada del personaje Marcio (*cfr.* De Valdés [0], p. 168).

[-1] Siempre sin ninguna intención de infringir el derecho de autoría, lo comparto con único propósito educativo e inspirador.

[○] *Vid. v. gr.* https://es.wikipedia.org/wiki/Número_de_Motzkin (imagen de de Mrmw, https://commons.wikimedia.org/wiki/File:Motzkin5.svg).

[1] *Vid.* https://commons.wikimedia.org/wiki/File:Vintage_Paper_Texture_(9789792113).jpg.

Nos hiciste para Ti,
Señor,
y nuestro corazón estará inquieto
hasta que no descanse en Ti.
(Agustín, *Confesiones*, I, 1).

Examínenlo todo y quédense con lo bueno.
(Pablo, *1Tes*, 5, 21).

Ustedes han recibido gratuitamente, den también gratuitamente.
(MATEO, 10, 8).

Gracias Señor por haberme permitido lograr ser Licenciado en Ciencias, sección Matemáticas —especialidad Estadística— por la Universidad de Málaga (UMA) y Doctor Ingeniero en Informática —especialidad Lenguajes y Sistemas Informáticos—[2] por la Universidad de Extremadura (UEx), y por llevar ejerciendo la docencia, en la enseñanza particular (1979–1987), en la reglada desde 1987 y en la universitaria desde enero de 1988, aún sin consunción. Lo cierto es que estos años sólo rubrican la existencia de experiencia en el camino, no más.

Estas notas están hechas desde la confianza en la enseñanza y la ayuda mutuas. De alguna u otra manera, varias generaciones de estimables *alumni*[3], en su mayoría de la Escuela Politécnica de la UEx, habéis trabajado con versiones anteriores de los temas de estas notas, en diversos formatos; os agradezco de corazón vuestro tiempo, la benevolencia y paciencia que habéis mostrado continuamente, vuestro aliento, desafío e influencia, así como el interés y la sinceridad en vuestras reacciones, y aunque nunca mi deuda estará saldada, espero haber sabido integrar éstas en mejoras en la exposición escrita y hablada de la materia, como siempre ha sido mi intención. Que lo haya conseguido o no queda a vuestro juicio.

Vaya mi agradecimiento también a mis apreciables colegas del Grupo de investigación de Ingeniería Telemática Aplicada y Comunicaciones Avanzadas (GÍTACA) por su magnífica disposición y ayuda ante las necesidades técnicas.

He sido afortunado de haber disfrutado de tan exquisito magisterio, siendo imposible su enumeración en estas líneas, menciono sólo a quienes han influido en algunos de mis intereses principales. De la etapa preuniversitaria: Francisco Javier CAMPOS Y FERNÁNDEZ DE SEVILLA, por su erre que erre día tras día fiel y vehemente por la lengua y la literatura; Emilio LASARTE VIDAL, por su entusiasmo por la física y por la vida; Pablo MAYO, por lo propio por la biología, y, en especial, Modesto GARCÍA GRIMALDOS, por sus valiosas orientaciones en la fe católica, y Antonio MUÑOZ AGUILERA, por cómo transmitía el rigor de la historia y su amor por la filosofía (*Scientia omnium rerum*...). De la etapa universitaria en la UMA: Rafael CONEJO RAMILO, por introducirme en el sinfín de problemas que estudia la programación matemática, la investigación operativa y la teoría de grafos; Francisco CRIADO TORRALBA, por iniciarme en la teoría de juegos; José Antonio CUENCA MIRA, por su ejemplo cotidiano de quehacer matemático; Juan Ignacio DOMÍNGUEZ MARTÍNEZ, por encaminarme extraordinariamente en la teoría de la probabilidad y en la teoría de los procesos estocásticos; Esperanza SÁNCHEZ CAMPOS por haber sido una excelente guía en la geometría, en la expresividad y en el poder de interpretación de ésta; Francisco SANZ por haber hecho lo propio en los mundos reales e imaginarios del

[2] *Vid*. LEÓN ROJAS (2003) [1].

[3] Latinismo (préstamo lingüístico) crudo no adaptado, alumnado. El constante rebitar machacón desde la *Magna Charta Universitatum* de 1988 de la palabra 'estudiante' parece perseguir la desnaturalización profunda del continuo enseñanza-aprendizaje y su colapso en una dimensión individualizada y afactorial, en un soliloquio de único protagonista el aprendizaje, en una muerte del profesorado hacia un renacer ideológico y postmodernista como agentes de formación, instrucción, facilitación, mediación, fomento, o vaya usted a saber qué. Sin alumnado no hay profesorado y sin profesorado no hay alumnado; sin embargo, sin profesorado sí que puede haber estudiantado. De aquí que prefiera hablar de 'alumnado' a 'estudiantado'. Además, hablando en plata y de corazón, por lo general, el profesorado, más allá de la servidumbre, procuramos ayudar en lo que conocemos; alumnado: acudid siempre que lo necesitéis.

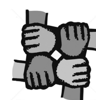
álgebra; Alberto de la TORRE RODRÍGUEZ por adentrarme en el análisis y cálculo numéricos; a él y a César RODRÍGUEZ ORTIZ por fomentar mi dedicación a las ciencias e ingeniería de la computación, y, en especial, a Francisco Javier GIRÓN GONZÁLEZ-TORRE, quien me abrió las puertas del razonamiento bayesiano y de la teoría de la decisión en general. De mis colegas de la UEx, cada día sigo aprendiendo.

No puedo obviar consignar aquí mi gratitud hacia quienes escribieron los textos de los cuales me he servido, algunos recogidos en la bibliografía.

¿Y cómo olvidarme de *la tribu*? Mi reconocimiento por el regalo de su tiempo, su invaluable experiencia y valiosa sabiduría. Cada día parece más evidente que el conocimiento nace de lo común. ¡GNU tribu![4, 5]

Deseo recordar aquí con especial gratitud y admiración a mi inolvidable amigo Domingo GUTIÉRREZ BARRANCO, quien me transmitió su amor por el conocimiento, su fascinación por la lógica y la filosofía, su pasión por la fe católica, la teología y en particular, la patrística y la escatología, y me inició en el desbrozo de tantos y tantos caminos a través de los muchos entresijos que las entreveran.

Doy las mayores gracias a mi compañera de vida y camarada MONTAÑA, *mi Musa*, a esa alma inquieta, curiosa y creativa, fuerte y a la par flexible, perseverante y capaz de reinventarse infinitamente; se las doy por su paciencia y comprensión, por su aliento, apoyo y ayuda en tantísimas situaciones y circunstancias y por continuar trayendo tanta inspiración, aventura y felicidad a mi existencia.



Juan Miguel LEÓN ROJAS,
septiembre de 2023.

[4] Por un lado, en mis caminatas por el mundo del conocimiento libre (*vid. v. gr.* https://es.wikipedia.org/wiki/Conocimiento_libre), conocí GNU (*vid. v. gr.* https://en.wikipedia.org/wiki/GNU); éste es un acrónimo recursivo de *GNU's Not Unix!* (GNU no es Unix) —y con razón de ser en que el diseño de GNU es similar al de Unix, si bien aquél es software libre y no contiene código de éste—. Por otro, la trigésimo tercera novela del *Mundodisco* de Terry PRATCHETT, *Going Postal* (*vid. v. gr.* https://en.wikipedia.org/wiki/Going_Postal), narra la creación de un sistema de torres de comunicación (los *clacks*), y cuando John Dearheart —hijo del inventor de dicho sistema, Robert Dearheart— es asesinado, Robert escribe un fragmento de código llamado «GNU John Dearheart» para que su nombre resuene por todas las líneas de comunicación: 'G' significa enviar a todas partes (pasarlo) (*General broadcast* [*Go forward*]), 'N' significa no registrado (*Not logged*) y 'U' significa enviar de vuelta al llegar al final de la línea (*tUrn around*) (como la recursividad del acrónimo GNU); en fin, esto hace que el nombre de John Dearheart se repita sin fin en todo el sistema porque: «*"Haven't you ever heard the saying 'Man's not dead while his name is still spoken'?"* ["¿Nunca has oído el dicho 'el hombre no muere mientras se siga pronunciando su nombre'?"]» (Grandad [justo al final del capítulo 4]). Así que: ¡GNU tribu!

[5] Por otra parte, muchos encuentros son inolvidables, algunos te seducen, otros logran que te enamores —incluso aunque sea por un camino largo y a las veces tortuoso, entre el enamoramiento y la limerencia, permaneciendo en ti un *douleur exquise* a resto abierto—, y otros, a causa de no sabes qué, simplemente, permanecen en tu memoria. Hablando de Terry PRATCHETT, el comienzo de *Dodger* (Perillán, en español) (*vid. v. gr.* https://en.wikipedia.org/wiki/Dodger_(novel)) —novela que no es del *Mundodisco*— es uno de estos encuentros: *The rain poured down on London so hard that it seemed that it was dancing spray, every raindrop contending with its fellow for supremacy in the air and waiting to splash down* [La lluvia caía con tanta fuerza sobre Londres que parecía un aerosol danzante, cada gota rivalizando con su compañera por la supremacía en el aire y esperando el momento de salpicar desde el suelo].

Índice general

Este índice no se cita a sí mismo. Como quizás veamos, es mucho mejor evitar cualquier autorreferencia. O, al menos, hemos de aprender a manejarlas con sumo cuidado. (Por cierto, si quisiésemos profundizar en mundos habitados por la autorreferencia, un magnífico punto de partida es el estudio de HOFSTADTER [2]).

C — Álgebra abstracta 832

Notación

Quien lee estas notas quizás quisiese echar un vistazo antes de nada a la siguiente notación.

Abreviaturas y siglas

AIC	actividad intermedia de cualificación.
CEOV	cuestión cuya entrega resuelta fue optativa y voluntaria.
c.r.a.	con respecto a; relacionado con.
Cubit	cuaderno de bitácora.
EFE	examen final extraordinario.
EFEC	examen final extraordinario para coincidencias.
EFO	examen final ordinario.
EPF	examen preparatorio final.
PEP	primer examen preparatorio.
p.h.e.c.	para hacer en casa.
RUD	red universal digital.
s.a.	sujeto a.
SEL	selección de cuestiones.
SEP	segundo examen preparatorio.
TT	tipo test.

Lógica matemática

Sigue una lista de signos atinentes a la lógica.

Σ	alfabeto.

Σ^*	lenguaje universal de alfabeto Σ (conjunto de palabras formadas por letras de Σ).
$\leftrightharpoons$	definidor.
$\bot$	contradicción.
$\top$	tautología.
$\neg$	negador.
id	afirmador.
$\vee$	disyuntor.
$\wedge$	conjuntor.
$\veebar$	contravaledor
$\rightarrow$	implicador.
$\leftarrow$	replicador.
$\nrightarrow$	desimplicador.
$\nleftarrow$	desreplicador.
$\leftrightarrow$	coimplicador.
$\mid$	incompatibilizador.
$\downarrow$	negador conjunto.
$\mathcal{L}_0$	lenguaje de la lógica de juntores.
$\Phi(\mathcal{L}_0, \mathcal{C})$	Conjunto de fórmulas de $\mathcal{L}_0$ generada por $\mathcal{C}$.
S_ϕ	conjunto de subfórmulas de ϕ.
T_ϕ	árbol-fórmula de ϕ.
V_ϕ	conjunto de variables proposicionales que aparecen en ϕ.
$\mathcal{F}_0$	conjunto de todas las fórmulas de la lógica de juntores.
$\mathcal{J}$	conjunto de los 16 juntores diádicos $\{\bot, \mathrm{id}_0, \mathrm{id}_1, \neg_0, \neg_1, \vee, \wedge, \veebar, \rightarrow, \leftarrow, \nrightarrow, \nleftarrow, \leftrightarrow, \mid, \downarrow, \top\}$.
$\mathcal{V}$	conjunto de las variables proposicionales.
$[\![\phi]\!]$	valor de verdad de la fórmula ϕ.
$I_w(\phi)$	valor de verdad de ϕ según la interpretación w; también lo notamos $[\![\phi]\!]_w$.

$\mathcal{M}(\phi)$ conjunto de todos los modelos para la fórmula ϕ.

$\mathcal{M}(\Phi)$ conjunto de todos los modelos para el conjunto de fórmulas Φ.

$\mathcal{C}(\phi)$ conjunto de todos los contramodelos para la fórmula ϕ.

$\mathcal{C}(\Phi)$ conjunto de todos los contramodelos para el conjunto de fórmulas Φ.

sgn función signo de una variable proposicional.

$\vDash$ deductor semántico (implicador lógico) (o, sinónimamente, doble trinquete); es llamada *implicación tautológica* en los textos en los que se denomina *implicación lógica* a $\Rightarrow$.

$\Dashv$ replicador lógico; es llamada *replicación tautológica* en los textos en los que se denomina *replicación lógica* a $\Leftarrow$.

$\Dashv\vDash$ codeductor semántico (coimplicador lógico).

$\vdash$ deductor (sintáctico) (o, sinónimamente, trinquete).

$\dashv\vdash$ codeductor (sintáctico).

$\forall$ generalizador (cuantor universal); en algunos textos se nota $\bigwedge$ o Π; su negación ($\neg\forall$) se nota a veces por $\not\forall$ o por $\overline{\forall}$.

$\exists$ particularizador (cuantor existencial); en algunos textos se nota $\bigvee$ o Σ; su negación ($\neg\exists$) se nota a veces por $\nexists$ o por $\overline{\exists}$.

$\exists!$ singularizador (cuantor de existencia única); su negación ($\neg\exists$) se nota a veces por $\not\exists!$ o por $\overline{\exists!}$.

$\exists^\circ$ función cuantorial de existencia no global; su negación ($\neg\exists^\circ$) se nota a veces $\not\exists^\circ$ o por $\overline{\exists^\circ}$.

$\therefore$ luego/por lo que/por lo tanto.

$\because$ porque/pues/puesto que/ya que.

$\mapsfrom$ operación *sustitución* (o, sinónimamente, *reemplazo* o *asignación*); $x \mapsfrom y$ significa que el valor actual de x se reemplaza por el valor actual de y sin modificar este último.

Γ_ϕ (o simplemente, Γ, si no ha lugar a confusión); siendo ϕ la fórmula $\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \rightarrow \psi$, Γ es un conjunto decisor de ϕ, esto es, un conjunto tal que se satisface que w es un modelo para Γ si, y sólo si, w es un contramodelo para ϕ.

T_Γ árbol semántico para Γ.

ρ_0 tronco de un árbol semántico dado.

ρ rama genérica de un árbol semántico dado.

ρ_i $(0 < i)$ rama iésima de un árbol semántico dado.

$\Rightarrow$ implicador/deductor/inferidor natural; corresponde al «si …, entonces …» (o, sinónimamente, al «…sólo si …» o al «…implica …») de la lengua natural; es llamada *implicación lógica* en los textos en los que se denomina *implicación tautológica* a $\models$.

$\Leftarrow$ replicador; corresponde al «…si …» de la lengua natural; es llamada *replicación lógica* en los textos en los que se denomina *replicación tautológica* a $\dashv$.

$\Leftrightarrow$ coimplicador/codeductor/coinferidor natural; corresponde al «…si, y sólo si …» de la lengua natural.

$\mathcal{L}_1^=$ lenguaje de primer orden con identidad.

ι descriptor definido.

$\mathcal{L}_1^+$ extensión aritmética, con las operaciones $+$ y $\cdot$, del lenguaje de primer orden con identidad $\mathcal{L}_1^=$.

N recuento cuantificado.

$^1/_2$ notación de la incertidumbre en una lógica trivalente; en algunos textos se nota con el signo de interrogación ?

L_n lógica de n-valores $(2 \leq n)$ de Łukasiewicz.

T_n conjunto $\{0, 1/(n-1), 2/(n-1), \ldots, (n-1)/(n-1)\}$ de números racionales de $[0, 1]$ en el que solían valorarse las lógicas de n-valores en los años treinta.

T_∞ conjunto de todos los números racionales de $[0, 1]$.

L_∞ lógica infinitamente valorada en el conjunto T_∞; extensión de la lógica estándar L_1 de Łukasiewicz.

Teoría de conjuntos

Sigue una lista de signos atingentes a la teoría de conjuntos.

V la clase universal (el universo de todos los conjuntos): $V = \{x : \top\}$.

R la clase de Russell: $R = \{x : x \notin x\}$.

$\{\,\}$ llaves de apertura y cierre de un conjunto en su definición por extensión.

$\{\{\,\}\}$ llaves de apertura y cierre de un multiconjunto en su definición por extensión.

$:$ definidor de los elementos de un conjunto; se lee «tal que»; por ejemplo, $\{x : \text{Madre}(\text{M}, x)\}$; en algunos textos aparecen otros signos con el mismo significado: $|$, $/$, $\backepsilon$.

$\in$ pertenencia de un elemento a un conjunto, por ejemplo, $-23 \in \mathbb{Z}$.

$\notin$ no pertenencia de un elemento a un conjunto, por ejemplo, $-23 \notin \mathbb{N}$.

μ_X función característica (o, sinónimamente, función indicadora, indicatriz, de pertenencia o de membresía) de X.

$\subseteq$ inclusión entre conjuntos; por ejemplo, $\mathbb{N} \subseteq \mathbb{N} \subseteq \mathbb{Z}$; cuidado, pues en algunos textos aparece el signo $\subset$ con el mismo significado.

$\nsubseteq$ no inclusión entre conjuntos; por ejemplo, $\mathbb{Z} \nsubseteq \mathbb{N}$.

$\subset$ inclusión propia entre conjuntos; por ejemplo, $\mathbb{N} \subset \mathbb{Z}$; en algunos textos aparecen otros signos con el mismo significado: $\subsetneq$, $\varsubsetneq$, $\subsetneqq$.

$\emptyset$ el conjunto vacío (asumimos que este conjunto existe; observemos que: 0.º, ninguna entidad es elemento del vacío, esto es, $x \notin \emptyset$, sea lo que sea x, y 1.º, $\forall C,$ conjunto, $\emptyset \subseteq C$.

$\mathcal{U}$ el conjunto universal; observemos que: 0.º, toda entidad es elemento del conjunto universal, esto es, $x \in \mathcal{U}$, sea lo que sea x, y 1.º, $\forall C,$ conjunto, $C \subseteq \mathcal{U}$.

2^C el *conjunto potencia* de un conjunto C, es el conjunto de todos los subconjuntos de A, $2^C = \{S : S \subseteq C\}$; alternativamente lo designamos por $\mathcal{P}(C)$.

$\cup$ unión de conjuntos.

$\cap$ intersección de conjuntos.

$\setminus$ diferencia de conjuntos; $X \setminus Y$ designa el conjunto $\{x : x \in X \text{ y } x \notin Y\}$; alternativamente usaremos el signo $-$ en vez de la barra inversa $\setminus$.

$\times$ producto cartesiano; $X \times Y$ designa el conjunto $\{\langle x, y\rangle : x \in X \text{ e } y \in Y\}$.

^{n} producto cartesiano de X por sí mismo n veces.

$\bigtimes$ $\bigtimes_{i=m}^{n} X_i$ designa el producto cartesiano $X_m \times X_{m+1} \times \cdots \times X_n$.

$^\complement$ complemento; $X^\complement$ designa el conjunto complementario (en el universal) de X.

$\hookrightarrow$ inyectividad; $f : X \hookrightarrow Y$ significa que f es inyectiva de X a Y; en algunos textos aparece el signo $\rightarrowtail$ con el mismo significado.

$\twoheadrightarrow$ sobreyectividad; $f : X \twoheadrightarrow Y$ significa que f es sobreyectiva de X a Y.

$\hookrightarrow\!\!\!\!\twoheadrightarrow$ biyectividad; $f : X \hookrightarrow\!\!\!\!\twoheadrightarrow Y$ significa que f es biyectiva de X a Y.

$|\ |$ cardinal; $|X|$ designa el cardinal del conjunto X; son de utilización frecuente los signos alternativos $\#X$ y $\operatorname{card} X$.

$\approx$ equipotencia; $X \approx Y$ designa la equipotencia de X e Y.

Rel_X el conjunto de todas las relaciones diádicas en X; lo designamos alternativamente por 2^{X^2}.

id_X la relación identidad en X, esto es, la endorrelación $I_X = \{\langle x, x\rangle : x \in X\}$.

$\mathbb{B}^n$ bola unidad (cerrada) de n dimensiones, $\mathbb{B}^n = \{d(x, 0) \leq 1\}$. (Es el círculo en el plano euclideo).

$\mathbb{D}$ disco unidad (o bola unidad abierta) de n dimensiones, $\mathbb{D}^n = \{id(x, 0) < 1\}$. (En el plano cartesiano las bolas se suelen llamar discos).

$\mathbb{S}$ esfera unidad de n dimensiones, $\mathbb{S}^n = \{d(x, 0) = 1\}$. (Es la circunferencia en el plano euclideo).

Sistema numérico

$\mathbb{N}$ conjunto de los *números naturales*, $\{0, 1, 2, 3, \ldots\}$; en algunos textos, 0 no se considera un número natural y se refieren a este conjunto como $\mathbb{N}_0$; también podremos referirnos a él como el conjunto de los *números enteros no negativos* (mayores o iguales que cero) ($\mathbb{Z}_0^+$).

$\mathbb{N}_n$ conjunto de los primeros n números naturales, $\mathbb{N}_n = \{0, 1, \ldots, n-1\}$; en algunos textos se nota $[n]$.

$\mathbb{N}_n^+$ conjunto de los primeros n números naturales positivos, $\{1, \ldots, n\}$; ; en algunos textos se nota $[n]^+$.

$\mathbb{P}$ El conjunto de los *números primos*, $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$.

$\mathbb{N}_{>k}, \mathbb{N}_{\geq k}$ respectivamente: $\{n \in \mathbb{N} : n > k\}$ y $\{n \in \mathbb{N} : n \geq k\}$; también se notan $(k, \rightarrow)_{\mathbb{N}}$ y $[k, \rightarrow)_{\mathbb{N}}$.

$\mathbb{N}_{<k}, \mathbb{N}_{\leq k}$ respectivamente: $\{0, 1, \ldots, k-1\}$ y $\{0, 1, \ldots, k\}$; también se notan $(\leftarrow, k)_{\mathbb{N}}$ y $(\leftarrow, k]_{\mathbb{N}}$.

$\mathbb{N}_{(h,k)}, \mathbb{N}_{[h,k]}$ respectivamente: $\{n \in \mathbb{N} : h < n < k\}$ y $\{n \in \mathbb{N} : h \leq n \leq k\}$; también se notan $(h, k)_{\mathbb{N}}$ y $[h, k]_{\mathbb{N}}$.

$\mathbb{N}_{(h,k]}, \mathbb{N}_{[h,k)}$ respectivamente: $\{n \in \mathbb{N} : h < n \leq k\}$ y $\{n \in \mathbb{N} : h \leq n < k\}$; también se notan $(h, k]_{\mathbb{N}}$ y $[h, k)_{\mathbb{N}}$.

$\mathbb{Z}$ conjunto de los *números enteros*, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

$\mathbb{Z}_{>k}, \mathbb{Z}_{\geq k}$ respectivamente: $\{n \in \mathbb{Z} : n > k\}$ y $\{n \in \mathbb{Z} : n \geq k\}$; también se notan $(k, \rightarrow)_{\mathbb{Z}}$ y $[k, \rightarrow)_{\mathbb{Z}}$.

$\mathbb{Z}_{<k}, \mathbb{Z}_{\leq k}$ respectivamente: $\{n \in \mathbb{Z} : n < k\}$ y $\{n \in \mathbb{Z} : n \leq k\}$; también se notan $(\leftarrow, k)_{\mathbb{Z}}$ y $(\leftarrow, k]_{\mathbb{Z}}$.

$\mathbb{Z}_{(h,k)}, \mathbb{Z}_{[h,k]}$ respectivamente: $\{n \in \mathbb{Z} : h < n < k\}$ y $\{n \in \mathbb{Z} : h \leq n \leq k\}$; también se notan $(h, k)_{\mathbb{Z}}$ y $[h, k]_{\mathbb{Z}}$.

$\mathbb{Z}_{(h,k]}, \mathbb{Z}_{[h,k)}$ respectivamente: $\{n \in \mathbb{Z} : h < n \leq k\}$ y $\{n \in \mathbb{Z} : h \leq n < k\}$; también se notan $(h, k]_{\mathbb{Z}}$ y $[h, k)_{\mathbb{Z}}$.

$\mathbb{Q}$ conjunto de los *números racionales*, $\mathbb{Q} = \{p/q : p \in \mathbb{Z} \wedge q \in \mathbb{Z}^+\}$; también utilizamos las notaciones $\frac{p}{q}$, ${}^{p}/{}_{q}$ y p/q).

$\mathbb{Q}_{>k}, \mathbb{Q}_{\geq k}$ respectivamente: $\{n \in \mathbb{Q} : n > k\}$ y $\{n \in \mathbb{Q} : n \geq k\}$; también se notan $(k, \rightarrow)_{\mathbb{Q}}$ y $[k, \rightarrow)_{\mathbb{Q}}$.

$\mathbb{Q}_{<k}, \mathbb{Q}_{\leq k}$ respectivamente: $\{n \in \mathbb{Q} : n < k\}$ y $\{n \in \mathbb{Q} : n \leq k\}$; también se notan $(\leftarrow, k)_{\mathbb{Q}}$ y $(\leftarrow, k]_{\mathbb{Q}}$.

$\mathbb{Q}_{(h,k)}, \mathbb{Q}_{[h,k]}$ respectivamente: $\{n \in \mathbb{Q} : h < n < k\}$ y $\{n \in \mathbb{Q} : h \leq n \leq k\}$; también se notan $(h, k)_{\mathbb{Q}}$ y $[h, k]_{\mathbb{Q}}$.

$\mathbb{Q}_{(h,k]}, \mathbb{Q}_{[h,k)}$ respectivamente: $\{n \in \mathbb{Q} : h < n \leq k\}$ y $\{n \in \mathbb{Q} : h \leq n < k\}$; también se notan $(h, k]_{\mathbb{Q}}$ y $[h, k)_{\mathbb{Q}}$.

$\mathbb{R}$ conjunto de los *números reales*, que además de incluir a $\mathbb{Q}$ contiene números como $\sqrt{2} = 1{,}414213562373095\ldots$ (constante de PITÁGORAS), $\sqrt[3]{2} = 1{,}259921049894873\ldots$ (constante de Delos[6]), $\phi = 1{,}6180339887498895\ldots$ (número áureo), $e = 2{,}718281828459045\ldots$ (número de EULER, constante de NAPIER), $\pi = 3{,}141592653589793\ldots$ (constante de ARQUÍMEDES, constante de LUDOLPH), etc.

$\mathbb{R} \setminus \mathbb{Q}$ conjunto de los *números irracionales*, $\mathbb{R} \setminus \mathbb{Q} = \{x : x \in \mathbb{R} \wedge x \notin \mathbb{Q}\}$; en algunos textos se nota $\mathbb{I}$.

$\mathbb{N}^*, \mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*$ respectivamente: conjunto de los números *naturales no nulos*, *enteros no nulos*, *racionales no nulos* y *reales no nulos*.

$\mathbb{N}^+, \mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$ respectivamente: conjunto de los números *naturales positivos*, *enteros positivos*, *racionales positivos* y *reales positivos*. (En algunos textos, los elementos de estos conjuntos se denominan «estrictamente positivos», llamándose allí positivos a los de que llamamos aquí no negativos). $\mathbb{N}^+$ no es otro que $\mathbb{N}^*$ (números na-

[6] El nombre hace referencia al oráculo de la isla de Delos.

turales no nulos, o sea, distintos de cero); en realidad, siempre que no sea por motivos pedagógicos nos referiremos a él como $\mathbb{Z}^+$.

$\mathbb{Z}_0^+, \mathbb{Q}_0^+, \mathbb{R}_0^+$ respectivamente: conjunto de los números *enteros no negativos*, *racionales no negativos* y *reales no negativos*.

$\mathbb{Z}^-, \mathbb{Q}^-, \mathbb{R}^-$ respectivamente: conjunto de los números *enteros negativos*, *racionales negativos* y *reales negativos*.

$\mathbb{Z}_0^-, \mathbb{Q}_0^-, \mathbb{R}_0^-$ respectivamente: conjunto de los números *enteros no positivos*, *racionales no positivos* y *reales no positivos*.

$\mathbb{C}$ conjunto de los números complejos.

$\mathbb{A}$ conjunto de los números algebraicos, subconjunto de $\mathbb{C}$, que contiene a todos los racionales y a números como $\sqrt{2}$, $\sqrt[3]{2}$, ϕ, $i = \sqrt{-1}$, etc.

$\mathbb{C} \setminus \mathbb{A}$ conjunto de los números trascendentes, que contiene números como $2^{\sqrt{2}} = 2{,}665144142690225\ldots$ (constante de GELFOND-SCHNEIDER), e, pi, $e^{\pi} = 23{,}140692632779269\ldots$ (constante de GELFOND), etc.

Álgebra abstracta

Sigue un compendio de los signos concernientes al álgebra abstracta que usamos en estas notas.

x' simétrico de x en

$\preceq$ ordenación.

$+$ indicador del conjunto de elementos positivos de un anillo ordenado; por ejemplo, $\mathbb{Z}^+$ (enteros positivos) del anillo ordenado $\langle \mathbb{Z}; +, \cdot \rangle$ de los enteros, $\mathbb{Q}^+$ (racionales positivos) del anillo ordenado $\langle \mathbb{Q}; +, \cdot \rangle$ de los racionales o $\mathbb{R}^+$ (reales positivos) del anillo ordenado $\langle \mathbb{R}; +, \cdot \rangle$ de los reales. También se designa en el subíndice, esto es, $_-$; en estos ejemplos, $\mathbb{Z}_-$, $\mathbb{Q}_-$ y $\mathbb{R}_-$.

$-$ indicador del conjunto de elementos negativos de un anillo ordenado.

$\operatorname{cinf}(B, A)$ conjunto de cotas inferiores de B en A.

$\operatorname{csup}(B, A)$ conjunto de cotas superiores de B en A.

$\operatorname{ínf}(B, A)$ ínfimo de B en A.

$\sup(B, A)$ supremo de B en A.

$\operatorname{mín}(B, A)$ mínimo de B en A.

$\operatorname{máx}(B, A)$ máximo de B en A.

$\sqcap$	operación *meet* de un retículo.
$\sqcup$	operación *join* de un retículo.
C_n	grupo cíclico de orden n.
S_n	grupo simétrico de orden n.
K_4	grupo de KLEIN (grupo cuadrático o del rectángulo, también denotado V_4 —*Vierergrupe* de KLEIN—).
D_3	grupo diédrico (de las isometrías que dejan invariable el triángulo equilátero en el plano euclideo) (grupo del triángulo).
D_4	grupo diédrico (de las isometrías que dejan invariable el cuadrado en el plano euclideo) (grupo del cuadrado).
Q_8	grupo de cuaterniones.

Teoría de números elemental

Sigue un compendio de los signos concernientes a la teoría de números que usamos en estas notas.

$\sum_{i=s}^{t} x_i$	*adición reiterada* $x_s + x_{s+1} + \cdots + x_t$.
$\prod_{i=s}^{t} x_i$	*producto reiterado* $x_s \cdot x_{s+1} \cdot \cdots \cdot x_t$.
$d \mid n$	d divide a n.
$D(n)$	conjunto de los *divisores positivos* de n $(n \in \mathbb{Z}^*)$.
$n\mathbb{Z}$	conjunto de los *múltiplos* de n $(n \in \mathbb{Z})$.
$n\mathbb{Z}^+, M(n)$	conjunto de los *múltiplos positivos* de n $(n \in \mathbb{Z}^*)$.
$n\mathbb{Z}_0^+, M_0(n)$	conjunto de los *múltiplos no negativos* de n $(n \in \mathbb{Z})$.
div	cociente de la división euclidea.
mód	resto de la división euclidea.
mcd	máximo común divisor.
mcm	mínimo común múltiplo.
$y \propto x$	y es directamente proporcional a x, esto es, existe $k \in \mathbb{R}^+$ tal que $y = kx$.
$\equiv \pmod{m}$	congruencia módulo m.

μ	función de MÖBIUS.
φ	función indicatriz de EULER.
σ_α	función divisor.
$\mathbb{Z}/m\mathbb{Z}$	enteros módulo m, esto es, del conjunto cociente $\mathbb{Z}/_{(\mathrm{mod}\ m)}$, es decir, de $\{[0]_m, [1]_m, \ldots, [m-1]_m\}$ (o, entendiendo que son clases de equivalencia, $\{0, 1, \ldots, m-1\}$).
$\mathbb{Z}_m$	abreviatura de $\mathbb{Z}/m\mathbb{Z}$.
$+_n$	suma en $\mathbb{Z}_n$; si no ha lugar a confusión, notaremos $+$.
$-_n$	diferencia en $\mathbb{Z}_n$; si no ha lugar a confusión, notaremos $-$.
$\cdot_n$	producto en $\mathbb{Z}_n$; si no ha lugar a confusión, notaremos $\cdot$.
$-a$	simétrico aditivo de a en $\langle\mathbb{Z}_m; +\rangle$, esto es, si, y sólo si, $a + (-a) \equiv 0 \pmod{m}$.
a^{-1}	simétrico multiplicativo de a en $\langle\mathbb{Z}_m; \cdot\rangle$, esto es, si, y sólo si, $a \cdot a^{-1} \equiv 1 \pmod{m}$.
$\mathbb{Z}_m^\times$	conjunto de los elementos multiplicativamente simetrizables de $\mathbb{Z}_m$; en la literatura figuran dos designaciones más con relativa frecuencia: $(\mathbb{Z}/m\mathbb{Z})^\times$ y $\mathbb{Z}_m^*$ (que en tales textos no debemos confundir con $\mathbb{Z}_m^* \setminus \{0\}$).
$t(m)$	conjunto de los enteros positivos menores que m que son coprimos con m, esto es, $\{k \in \mathbb{Z}^+ : 1 \leq k < m, \mathrm{mcd}(k, m) = 1\}$; en inglés, estos números son conocidos como los *totatives* de m.

Razonamiento combinatorio

$\lfloor x \rfloor$	suelo de x.
$\lceil x \rceil$	techo de x.
$\lfloor x \rceil$	redondeo de x.
$[x]$	truncamiento de x.
$n!$	factorial de n.
$n^{\underline{k}}$	factorial descendente de n de orden k.
$n^{\overline{k}}$	factorial ascendente de n de orden k.
$p_n\#$	primorial del número primo p_n.
$n\#$	primorial del número entero positivo n.

$\binom{n}{k}$	coeficiente binomial.
$\binom{n}{k_0, k_1, \ldots, k_p}$	coeficiente multinomial.
$V(n.k)$	número de variaciones de k elementos de un conjunto de n elementos.
$VR(n.k)$	número de variaciones con repetición de k elementos de un conjunto de n elementos.
$P(n)$	número de permutaciones de los n elementos de un conjunto de n elementos.
$\overset{\circ}{P}(n)$	número de permutaciones circulares de los n elementos de un conjunto de n elementos.
$C(n,k)$	número de combinaciones de k elementos de un conjunto de n elementos.
$CR(n,k)$	número de combinaciones con repetición de orden k de un conjunto de n elementos.
$\#S$	número de formas en que sucede el suceso S o número de formas de realizar la fase S.
$S(k,r)$	número de Stirling de 2.ª especie.
$\Sigma(k,n)$	$= \sum_{i=1}^{n} S(k,i)$; en algunos textos, $\Sigma(k,n)$ se nota por $S(k)$.
$p(k,r)$	$p(k,r) = p(k-1,r-1) + p(k-r,r)$ $(1 < r < k)$, con $p(0,0) = 1$ y $p(k,1) = p(n,n) = 1$ $(1 \leq k,n)$; $p(k,r)$ también se nota $p_k(r)$.
$\Pi(k,n)$	$= \sum_{i=1}^{n} p(k,i)$; $\Pi(n,n)$ suele designarse por $p(n)$; en algunos textos, $\Pi(k,n)$ se nota por $p(k)$.
$L(k,r)$	número de Lah sin signo; también llamado número de Stirling de 3.ª especie.
$A(k,n)$	$= \sum_{i=1}^{n} L(k,i)$; en algunos textos, $A(k,n)$ se nota por $L(k)$.

Ecuaciones en diferencias

S_n	suma parcial de los n primeros términos de una sucesión.
$F(n)$	término no homogéneo de una ecuación en diferencias.
F_n	enésimo número de FIBONACCI.
L_n	enésimo número de LUCAS.
T_n	enésimo número triangular.

J_n	enésimo número de JACOBSTHAL.
P_n	enésimo número de PELL.
${}_cP_1^{(2)}(n)$	enésimo número unigonal central.
p_n	enésimo número pentagonal.
${}_2p_n$	enésimo segundo número pentagonal.
${}_gp_n$	enésimo número pentagonal generalizado.
$Y_5^{(3)}(n)$	enésimo número piramidal cuadrado.
$L(x, y)_n$	enésimo número de PISOT $L(x, y)$.

Signos y símbolos auxiliares

 el *mochuelo de Atenea* es el ave que acompaña a Atenea, diosa de la sabiduría, entre otras cosas (*cfr. v. gr.* https://es.wikipedia.org/wiki/Mochuelo_de_Atenea); por si en alguna ocasión hubiese recurrido a él.

 tal como su propio nombre indica (enlace externo), este símbolo señala que lo que sigue es un enlace externo: lo uso ocasionalmente, ya que por lo general basta con la dirección de la página web; claro que visto el número de veces que lo he empleado, me veo en la obligación de apostillar que esto, en realidad, no es una impostura, sino un *acto de uso* («a la SEARLE [3]) del cero, del conjunto vacío o de la clase vacía, según se mire.

 una bolaspa en rojo: uso este signo para indicar un esquema argumental no válido.

 el símbolo de HALMOS (llamado, a veces, lápida [*tombstone*]) denota el fin de una demostración, Q. E. D. (*quod erat demonstrandum*) (cuando muestro más de una vía de demostración, uso también □).

 «Esta esperanza que nosotros tenemos, es como un ancla del alma, sólida y firme, que penetra más allá del velo, allí mismo donde Jesús entró por nosotros, como precursor, convertido en Sumo Sacerdote para siempre, según el orden de Melquisedec.» (Hebreos 6, 19–20).

Prólogo a las ediciones tercera y siguientes

No digáis que agotado su tesoro,
de asuntos falta, enmudeció la lira;
podrá no haber poetas; pero siempre
habrá poesía.

(Gustavo Adolfo BÉCQUER, *Rima IV*,
https://www.cervantesvirtual.com/obra-visor/rimas-y-leyendas--0/html/).

Del tiempo que no pasa.

Desde que apareció en su edición cero en septiembre de 2023, poco antes de su edición primera, aquella de enero de 2024, la segunda, en enero de 2025, la tercera, en mayo de 2025 y la cuarta, ésta que lees, recién brotada en estos días de enero de 2026, esta compilación de notas ha evolucionado en varios sentidos. Las he ido revisando, en ocasiones junto a ti, quien lees, si bien a veces sin ser conscientes de ello, ni tú ni yo. Te lo agradezco sobremanera. Las he corregido o modificado, abrotoñando ocasionalmente revisiones[7]. Algunas actividades han dejado de serlo, mudando en ejemplos. De otras, ha emergido un añadido, con miras a su resolución. He ampliado algunos capítulos, no sólo por aclarar lo confuso o enmendar erratas y errores, sino por incluir parte de lo olvidado; claro que únicamente de lo que me he percatado. Demasiadas cosas quedan aún en este tintero, pero ya sabes, tú, quien lees, el tiempo abre un montón de tinteros y la vida ofrece una superabundancia de tarros de miel. Dejo para ti toparte con las variaciones de estas notas: no es mi deseo privarte en este recorrido ni del placer del hallazgo ni del goce del encuentro; además, nunca hice cuentas de llevar la cuenta (para tales menesteres, soy más tardo que anheloso). Sea lo que fuere, por otra parte y, finalmente, nunca lo olvides, tú eres imprescindible. El tiempo no pasa sin ti.

JMLR[8].

[7] Las revisiones de una edición son copias exactas de ésta, salvo correcciones y añadiduras, menores o mayores, necesarias. Aparecen, sin previo aviso, en https://archive.org/details/leon-rojas-j.-m.-2024-cuestiones-de-matematicas-discretas.-volumen-0, sustituyendo a la que hubiese.

[8] https://archive.org/details/@juan_miguel_leon_rojas.

Prólogo a las ediciones cero a segunda

> Duke Ellington le dijo a Tony [Bennett]: «Número uno: nunca te rindas. Número dos: siempre escucha a la regla número uno».
>
> (Stefani Germanotta (Lady Gaga) (1986–),
> 32.ª edición anual de los *American Cinematheque Awards*, 29.11.2018,
> https://www.youtube.com/watch?v=fCtMV-YytR4&t=145s).

De unas primeras consideraciones y la materia que sigue.

Matemática y sociedad

Dicen las malas lenguas que las ocasiones de utilizar en la vida real los conocimientos matemáticos adquiridos son muy raras y que, aparte de sumar a dividir y la noción de proporcionalidad, las personas no tienen oportunidad de hacerlo. Por otro lado, algunas de ellas a las que les ha llegado el éxito social se jactan de no haber comprendido jamás la matemática.

Y es precisamente en la formación intelectual que aporta la enseñanza y aprendizaje de la matemática en lo que deberíamos insistir de cara a la sociedad: «que nadie entre aquí si no es geómetra» (entiéndase si no sabe matemática) decía Platón. Tampoco se trataría de formar profesionales de la matemática, pero la realidad es que casi sea cual sea la disciplina escogida, nos encontramos con el uso de ésta. Quienes se dedican a la literatura (gramática, fonética, lingüística), historia (cuantitativa), geografía, sociología, psicología, economía, física…, en algún u otro momento necesitan de la matemática. Todo esto dejando a un lado, aunque no desestimándolos, todos aquellos elementos de acción de la matemática en el área de las costumbres: orden, reflexión, prudencia, orden, ética y honradez.

En principio, una formación matemática aporta a la persona un enriquecimiento conceptual. Los conceptos de número, operación, verdad matemática, relación, proporción, y tantos otros, forman parte del bagaje intelectual personal moderno. Además, una formación matemática nos acostumbra a sobrepasar la realidad concreta para traducirla a una nueva lengua depurada, más abstracta, pero que hace aparecer las semejanzas entre situaciones aparentemente muy alejadas unas de otras. Esta aproximación de situaciones, este agrupamiento de problemas distantes, proporciona una gran potencia de razonamiento y permite descubrir las formas generales bajo las apariencias,

simplificando de alguna manera nuestra visión del mundo para dar a nuestra acción más fuerza y eficacia.

Subyacente en muchas situaciones se esconde una estructura matemática, siendo la puesta en evidencia de ésta uno de los objetivos de la formación matemática. Estudiar matemática es esencialmente aprender a razonar pero, sobre todo, habituarnos a tomar conciencia del propio razonamiento. Así pues, no se trata únicamente de adquirir hábitos de razonamiento correcto (lo cual es de por sí importante), sino de habituarnos a tomar conciencia de los propios pasos de nuestro pensamiento, y esto sean cuales sean las enormes dificultades que ello plantea. Las reglas del razonamiento matemático no son innatas, sino que exigen un cierto aprendizaje. Si bien es posible que el razonamiento deductivo sea mayoritario actualmente en nuestra sociedad, ésta está abierta, junto con la tecnología, a todo tipo de razonamiento.

Todo ello no se puede realizar sin un lenguaje particular capaz de conjuntar la precisión y la elegancia, la sobriedad y la densidad. Una buena formación matemática va acompañada automáticamente de la adquisición de una lengua depurada que gana en concisión sin suprimir por ello la belleza. La perfección de una demostración matemática depende a la vez del rigor del razonamiento como de la forma en que esta demostración se expresa.

Se comprende, pues, que una buena formación matemática es un elemento esencial de una buena adaptación a la vida actual. En nuestro mundo, prácticamente todo se reduce a cantidades, se expresa por resultados numéricos, por estadísticas. Al enseñar matemática, contribuimos a ese equipamiento intelectual necesario para que las personas participen en la vida ciudadana. Una buena formación matemática conlleva hacer descubrir una nueva forma de pensamiento, en proporcionar nuevas formas de presentar los ejemplos, cuestiones y actividades, y resolverlas. Enseñando matemática, enseñamos a descubrir la verdad oculta tras el argumento engañoso que se viste con cifras, distinguiendo lo que es posible afirmar con certeza y rigor de lo falso o aproximado. Reducir la enseñanza de la matemática a una simple técnica, supone no conocer ni reconocer toda su potencia y eficacia.

Presentación

Presento estas notas incompletas de clase (NIC) con varios temas introductorios[9] a la matemática discreta y a sus aplicaciones.

Aunque carecen de requisitos de conocimiento previo más allá de los preuniversitarios (he pretendido que los diferentes capítulos sean en gran medida autosuficientes, además de procurar que su presentación sea rigurosa pero sencilla[10]), puede que en ciertas ocasiones, haber trabajado deter-

[9] Si hemos hojeado estas NIC, habremos observado que están aún faltas de la incorporación o desarrollo de ciertos contenidos. Dios mediante, llegará su momento; la metalicencia ✝ Gratuidad Cristiana con la que se publican permite su adopción, revisión y republicación por terceras personas.

[10] Claro que a la contra pudiésemos consultar [4], repleto de enunciados sencillos y sus demostraciones, éstas en sus versiones lo más complicadas que se le ocurrió al autor.

minados conceptos de matemáticas (principalmente de álgebra, cálculo y probabilidad) y de computación (principalmente de programación —una subclase del álgebra—), facilite la enseñanza y aprendizaje de los enteramente nuevos.

Constituyen una republicación corregida y aumentada de materiales que anteriormente vieron la luz como notas de clase, exámenes y sus soluciones. Conservando los objetivos y la estructura profunda de estas anteriores ediciones suscintas no inéditas, en ésta intento corregir deficiencias detectadas e incluir nuevos temas y actividades.

Estas NIC, más en su volumen cero, no tienen ninguna pretensión de tratar todos los temas de la matemática discreta. He tenido en cuenta, entre otras y principalmente, las recomendaciones presentes en el informe *Computer Curricula* 2020 [5] y particularmente en el *Computer Engineering Curricula* 2016 [6] y en el *Computer Science Curricula* 2013 [7], sin olvidar las ya clásicas de Alfs Bertziss (1987) [8].[11]

En cuanto a matemática discreta, este último informe CSC identifica los siguientes temas como esenciales para las estructuras discretas (págs. 76–81): DS1) funciones, relaciones y conjuntos; DS2) lógica básica; DS3) técnicas de demostración; DS4) principios de recuento; DS5) grafos y árboles; DS6) probabilidad discreta. A los cuales añadiríamos: I, matrices (MAT); II, algoritmos y complejidad (AL), y III, teoría básica de números (NUM). Excepto DS5, DS6, MAT y AL, que aparecerán ocasionalmente, el resto se estudiará[12,13,14].

Esta selección y tratamiento de cuestiones básicas definen un marco para futuros refinamientos y extensiones y asientan el camino para el volumen uno de estas NIC, en el que se estudiarán otros

[11] En la presente edición se han revisado y contrastado con el *Computer Science Curricula 2023* (enero de 2024) (https://dl.acm.org/doi/pdf/10.1145/3664191) y con las fichas de recomendaciones de la CODDii (https://coddii.org/fichas).

[12] Hemos de tener en cuenta que DS5, DS6, MAT y AL se tratan en otras asignaturas de los planes de estudio actuales de los grados en ingeniería informática en la Escuela Politécnica: DS6, en UEX501270 Estadística (2.º semestre); MAT, en UEX502382 Álgebra lineal (1.er semestre); AL, en UEX502304 Introducción a la programación (1.er semestre) y en UEX501273 Análisis y diseño de algoritmos (3.er semestre); DS5, en esta última y en UEX501271 Estructuras de datos y de la información (2.º semestre), si bien desde un punto de vista algorítmico.

[13] La impartición que ha acompañado a estas NIC en la Escuela Politécnica de la Universidad de Extremadura (UEX501272 Ampliación de matemáticas, en el 2.º semestre) hasta el año académico 2025-2026, ha incluido además, cuando ha habido tiempo, unas más que brevísimas pinceladas sobre algunos métodos numéricos. Con respecto al cálculo numérico, identificamos como contenidos esenciales: I, raíces de ecuaciones (RE); II, ecuaciones algebraicas lineales (EAL), y III, ajuste de curvas (AC) (regresión e interpolación); lo cual nos proporciona una introducción suficiente a los algoritmos y métodos para la computación de aproximaciones discretas usados para resolver problemas continuos, tanto en el ámbito de lo lineal como de lo no lineal. Estudiamos sólo RE. Esto es así porque EAL y AC se tratan en otras asignaturas de los planes de estudio actuales de los grados en ingeniería informática en la Escuela Politécnica: EAL, en UEX502382 Álgebra lineal (1.er semestre); AC, en lo tocante a regresión, en UEX501270 Estadística (2.º semestre). Quizás algún contenido correspondiente a RE aparezca en una futura edición de estas NIC volumen cero o en su volumen uno. Agradecido en cualquier caso a la vida, pues vía esta impartición he aprendido y han surgido multitud de ideas y técnicas.

[14] En el año académico 2026–2027 se prevé un nuevo plan de estudios que conllevará la transformación de Ampliación de Matemáticas en la asignatura Matemática Discreta, con un plan docente común en el grado en ingeniería informática en la Escuela Politénica (EPCC) y en el Centro Universitario de Mérida (CUM) (cuatro menciones en la EPCC —Ingeniería del Software; Ingeniería de Computadores; Ciberseguridad, y Ciencia de Datos—, y dos menciones en el CUM —Tecnologías de la Información, e Inteligencia Artificial—), con los descriptores de contenidos: álgebra de Boole; aritmética; combinatoria, y grafos. Las futuras ediciones de estas NIC reflejarán la influencia de la impartición de dicha asignatura.

temas de la matemática discreta como: probabilidad discreta; grafos y árboles; teoría de autómatas; verificación de programas; complejidad algorítmica; computabilidad.

Como *objetivos* concretos tenemos los siguientes.

- *Dianas*.— ◎ Representación, ◎ formulación, ◎ abstracción, ◎ modelización, ◎ verificación y ◎ generalización.
- *Generales*.— • Adquirir cultura científica y cultura matemática en particular. • Potenciar las actitudes reflexivas y creativas. • Potenciar habilidades y destrezas de análisis, búsqueda, descubrimiento, verificación y generalización. • Promocionar el desarrollo y mejora de las habilidades de resolución de problemas y de las actitudes positivas hacia el pensamiento matemático, analítico, crítico concreto y creativo. • Mejorar la preparación para el estudio independiente y crítico y la capacidad de valoración de publicaciones académicas elementales y divulgativas sobre los contenidos tratados en la asignatura. • Desarrollar la capacidad de aprendizaje permanente.
- *Comunes*.— • Reconocer *patrones* y *estructuras*. • Potenciar la habilidad para elaborar *estrategias de resolución* de problemas y de *toma de decisiones*. • Incrementar la capacidad de *interpretación de los resultados* hallados y de *obtención de conclusiones*. • Aumentar el rigor en las argumentaciones y desarrollar las habilidades para usar la información y para la lectura y escritura y para la exposición oral o escrita de ideas y razonamientos.
- *Específicos de los temas de Fundamentos y de Teoría de números*.— • Potenciar la habilidad para comprender y usar el lenguaje lógico-matemático. • Desarrollar la capacidad de abstracción mediante la construcción y reconstrucción de argumentaciones lógico-matemáticas. • Potenciar la capacidad de razonamiento lógico-matemático en sus tipos deductivo, inductivo, abductivo y algorítmico.
- *Específicos de los temas de Razonamiento combinatorio y de Ecuaciones en diferencias*.— • Potenciar la capacidad de razonamiento lógico-matemático en sus tipos inductivo, algorítmico y recursivo. • Potenciar la habilidad para el recuento.

Profundizar en el desarrollo de estos objetivos pasa necesariamente por estudiar las referencias en las que se basan, en líneas generales, las materias que aquí se trabajan. Tengámoslo en cuenta.

Como *contenidos* tenemos los siguientes.

- Parte I.— Cimientos: lógica y análisis formal: lógica de juntores y de cuantores (cálculo; semántica; metalógica y demostraciones); lógica de clases; lógica de relaciones; lógica de funciones; lógica de lo infinito; lógica de conjuntos (axiomáticas); lógica de la construcción del sistema numérico; lógica inductiva; lógica de estructuras.
- Parte II.— Teoría de números elemental: divisibilidad; aritmética modular; primos y máximo común divisor; resolución de congruencias lineales y sus aplicaciones; ecuaciones diofánticas.

- Parte III.— Razonamiento combinatorio: principios fundamentales de recuento; operaciones combinatorias básicas (variaciones, permutaciones y combinaciones, sin y con repetición); demostraciones combinatorias; modelización de cuatro problemas combinatorios de recuento simples y operaciones combinatorias avanzadas.
- Parte IV.— Ecuaciones en diferencias: resolución de ecuaciones en diferencias lineales y de problemas de valores iniciales; sistemas dinámicos lineales discretos.

Dependiendo de la inquietud y tiempo de quien lee y estudia, pudiese ampliar, por su interés, con subtemas transversales, pues no son objeto de estudio directo en estas NIC, como los siguientes[15].

- Parte I.— Lógica borrosa; conjuntos borrosos; inteligencia artificial; sucesiones y sumas y matrices, incidiendo en las particularidades de lo discreto frente a lo continuo, fundamentalmente desde aspectos algorítmicos de su tratamiento numérico; teoría de la decisión; teoría de códigos.
- Parte II.— Temas de algoritmia, computabilidad, complejidad, computación simbólica, codificación de la información, verificación y seguridad computacional.
- Parte III.— Algún caso particular del teorema de RAMSEY; cuestiones de probabilidad discreta, optimización, programación entera, teoría de la información, árboles, teoría de grafos, redes —si bien incluyen estas NIC unos apuntes breves de estas tres—, datos masivos, aprendizaje automático y aprendizaje profundo.
- Parte IV.— Aspectos de recursividad; procesos estocásticos discretos; fractales; geometría computacional; simulación.

Ortografía, léxico, uso del español y ortotipografía

En otro orden de cosas, en cuanto a la *ortografía*, tal y como me enseñaron, escribo con tilde diacrítica *solo* sólo cuando es adverbio y sin tilde cuando es adjetivo (casi pudiésemos decir que sólo cuando va solo); con respecto a los demostrativos, los escribo sin tilde cuando son adjetivos y con tilde cuando son pronombres, salvo los neutros admitidos por el singular, *esto*, *eso* y *aquello*, que nunca llevan tilde, esto es, caso de ser pronombres, los tres, con sus formas femeninas y masculinas del singular y plural: 0.ª, éste, ésta, éstas, éstos; 1.ª, ése, ésa, ésas, ésos, y 2.ª, aquél, aquélla, aquéllas, aquéllos.

Respecto al *léxico* y *uso del español*, defiendo la terminación ‘se’ frente a ‘ra’ de los pretéritos imperfecto y pluscuamperfecto de subjuntivo, y con verbos modales como deber, poder, querer, saber o soler sabemos que es posible intercambiar el condicional simple y el pretérito imperfecto de subjuntivo, por lo que procuraré usar éste (salvo en casos de que quisiese reflejar un matiz de duda o eventualidad

[15] Siempre que he impartido estas NIC en la Escuela Politécnica de la Universidad de Extremadura (en la asignatura UEX501272 Ampliación de Matemáticas, en el 2.º semestre), he procurado incluirlas, si el tiempo lo ha permitido, entre clases, seminarios o laboratorios y un foro asíncrono de comunicación.

alternativa —esa incertidumbre que inspiramos con el subjuntivo o esa probabilidad o posibilidad que expresamos con el condicional frente a la certeza que manifestamos con el indicativo—), incluso a veces con el presente de indicativo con cierto tono cortés, eufemístico o irónico (por ejemplo, debiéseis estudiar por debéis estudiar).

Este uso también supedita la elección entre diferentes palabras o expresiones; a modo de ejemplo: inmediatamente anterior, precedente o retropróximo.

De ayuda son: el Diccionario de la lengua española[16] y los diferentes recursos en línea de la Real Academia Española[17].

Por otra parte, he intentado, por lo general, seguir las recomendaciones sobre *ortotipografía* de Javier Bezos en tex*nia*[18] (por lo general, porque todo estándar es cuestionable[19], si no por la presente, por alguna generación venidera). La *versión en* .pdf de estas notas pretende representar su papel de ayuda hipertextual con la matemática discreta. Los *cuadros*, *figuras*, *supuestos*, *teoremas*, *lemas*, *fórmulas* y *actividades*, los indico por dos números, el primero de los cuales hace referencia al capítulo y el segundo al orden de aparición en estas notas. Los *ejemplos*[20], sin embargo, los indico por un solo número; en cierta manera, esto invoca la continuidad y cohesión del contenido.

Cero es un número natural

Finalmente, decir que estoy entre las personas para quienes

cero es un número natural[21].

Y si hemos acudido adonde nos remite la anterior nota al pie, entendemos, ya que no sólo por donde he nacido[22]. En cuanto al ordinal de cero[23,24], si bien en inglés técnico es frecuente decir *zeroth*, en español pudiésemos leer «0.º» simplemente como cero, esto es, decir, por ejemplo, norma/principio/-regla cero; en lenguajes de programación es común hablar de que una entidad tiene un índice/valor

[16] https://dle.rae.es/.
[17] https://www.rae.es/recursos.
[18] https://www.texnia.com/.
[19] https://xkcd.com/927/.
[20] «Más vale el ejemplo que el consejo» (Paremia anónima). En estas notas, los ejercicios, sean instrumentales o no, y los problemas, enunciados en lenguaje lógico-matemático o en español, todos ellos, los denomino *ejemplos*, porque, en definitiva, eso es lo que son (aunque otras personas asegurarían que son «actividades resueltas»). Las *actividades* (de las que tales personas dirían que son «actividades propuestas») irán transformándose en ejemplos —pertinentes a su contexto— a medida que vaya teniendo tiempo de integrar su solución en futuras revisiones o ediciones de estas notas (lo mismo sucederá con las demostraciones faltantes de algunos lemas, proposiciones, teoremas y corolarios) —si bien en algunos casos quedarán en un estado intermedio, con indicaciones más o menos extensas «con miras a su resolución»—. A falta de una división explícita, diré que hay ejemplos y actividades que seguramente encuadraríamos en alguno de estos tres tipos: de comprobación, de aplicación y de ampliación.
[21] *Cfr. infra* § 15 (pág. 784 de esta edición).
[22] De manera natural, espontánea y tradicional, por aquí, en España, decimos planta cero o planta baja; incluso en inglés británico, *ground floor*, a diferencia de en Estados Unidos, que se dice *first floor* (primera planta).
[23] *Cfr. v. gr.* https://mdc.ulpgc.es/utils/getfile/collection/numeros/id/701/filename/701.pdf.
[24] *Cfr. v. gr.* http://akusmatika.org/wp-content/uploads/2019/02/seudonimo.pdf.

ordinal de cero y en psicometría de escala (de tipo) ordinal de cero a n, entre otros ejemplos[25]. También pudiésemos considerar usar el galicismo nuliemo (de *nullième*) o aventurarnos con cerésimo[26] o incluso con ceroésimo[27].

JMLR[28].

[25] *Cfr. v. gr.* https://www.babab.com/no06/fin_de_siglo.htm.

[26] *Cfr. v. gr.* https://diccet.com/2021/02/17/ceresimo-ceresima/.

[27] *Cfr. v. gr.* https://www.change.org/p/real-academia-española-que-la-rae-acepte-ceroésimo-como-el-ordinal-anterior-a-primero?source_location=topic_page.

[28] https://archive.org/details/@juan_miguel_leon_rojas.

Otro caso: Compro en un pueblo una instalación de luz eléctrica con la rebaja del 10 por 100.

—Mira, Pedro, que aquí faltan las bombillas.

—Bien, las desquitaremos al ajustar la cuenta: son diez luces que me costaron a diez pesetas, que hacen cien pesetas; te rebajo diez, y quedan en noventa.

—¿Y las bombillas?

—Eran diez. A peseta cada una, son diez pesetas. Rebaja el 10 por 100, y quedan en nueve pesetas. Desquita de noventa, y me das ochenta y una, y en paz.

—No, hombre; tú me das por noventa pesetas la instalación que tienes, y además diez bombillas que me cuesten nueve pesetas; y como en la tienda cuestan diez, me tienes que dar esas diez pesetas para que yo las compre, y una peseta más para que las compre con el 10 por 100 de ventaja. De modo que de noventa pesetas te desquito once.

—Pues no lo entiendo.

Silverio LANZA (seudónimo de Juan AMORÓS) [9]: págs. 37–39
—publicado previamente como parte del artículo El paletismo, en la revista *Alma Española* [10];
también lo recoge Rafael RODRÍGUEZ VIDAL [11]: pág. 116 (en: § Contabilidad rusticana)—.

Preámbulo. Del proceder

No desperdiciéis el tiempo, que pronto se desvanece. El orden os enseñará a aprovecharlo. Os aconsejo, pues, querido amigo, que entréis primero en el *Collegoium logicum*. Allí os peinarán el espíritu como es debido, os calzarán los borceguíes de la tortura, a fin de que se deslice con más cuidado por el sendero del pensamiento y no se tuerza a un lado y a otro y se descarríe.

(Johann Wolfgang GOETHE (1808) *Fausto*, 1.ª parte.
—Traducción de Miguel Ruiz Castillo;
Rodegar, Barcelona, 1969, pág. 63—).

De cómo se imagina quien escribe la enseñanza de la materia.

La matemática está repleta de puntos de comienzo —axiomas, postulados, definiciones, enunciados—, de desarrollo —principios, hipótesis, conjeturas, argumentos, premisas, demostraciones, conclusiones—, de resultado —lemas, proposiciones, teoremas, corolarios— y de aplicaciones en Ciencia, Tecnología y Sociedad[29] (CTS) y vuelta al principio, pues estas aplicaciones son excelentes puntos de comienzo. La transdisciplinariedad expresa impresa en la naturaleza de la matemática es la responsable. Si bien pudiésemos entretenernos en disquisiciones técnicas sobre la idoneidad de la salida y una supuesta llegada, nuestro objetivo está en el propio camino, en su traza vaga y en su recorrido personal.[30]

De hecho, a grandes rasgos, dos son las travesías que se nos presentan a la hora de enfrentar la resolución de cuestiones matemáticas: una, *informal*, dejándonos guiar en su mayor parte por nuestra *intuición*, y la otra, *formal*, en la que si bien en su inicio pudiésemos invocar a nuestra intuición, bien hiciésemos, por ser nuestro deber, en averiguar diversas formas de representar lógico-matemáticamente —lo que incluye su representación algebraico-computacional, siempre que sea posible— la cuestión a resolver y cómo modelizarla de manera ajustada a sus peculiaridades, de tal modo que una vez verificada nos provea de una solución que tenga hechura y que sepamos interpretar nosotras, las criaturas humanas.

[29] *Vid. v. gr.* https://es.wikipedia.org/wiki/Estudios_de_ciencia,_tecnología_y_sociedad.

[30] «Estudia con ahínco lo que más te interese de la forma más indisciplinada, irreverente y original posible» (Richard FEYNMAN).

No debiera ser nuestra meta convertirnos en personas hábiles en el citar y recitar definiciones, resultados y nombres[31]. Sí debiera ser descubrir cómo pensar.

Además de estudiar, meditar y enseñar, lo mejor para entender, discernir e inferir, es hacer, mostrando qué se hace, cómo se hace por qué se hace y, sobre todo, para qué se hace; mas también aunque no se muestre. Y nada se hace sin entusiasmo —«Es un signo de mediocridad ser incapaz de entusiasmarse» (*C'est un signe de médiocrité que d'être incapable d'enthousiasme*) (Honoré de BALZAC, *Maximes et pensées*, 1856)—, sin embargo, es quimérico reclamar lo que no nos pertenece. Hacer las cosas con alma es pensar primero en los demás, si cabe en la rendición de cuentas.

Hacer menos pero más intensa, reflexiva y eficientemente, aprendiendo qué debe priorizarse, o hacer más, individual o colectiva, confiada y solidariamente, simplemente porque así se desea. Sea como y por lo que fuere, el buen pensar y mejor hacer; que ya se dice por saberse. Perturbador anhelo, ¿verdad?

No son muchos los contenidos previos necesarios para el estudio de las materias que se tratan en estas notas. De hecho, éstas quieren ser autocontenidas en su pretensión tanto de ser una introducción a la matemática discreta como una exposición de, y a, ciertos resultados recientes.

Nuestro pensamiento tiene su inicio en la observación y, por eso, en su esencia, está determinado empíricamente. Comenzamos con el estudio de la *lógica*, siguiendo así el consejo de Mefistófeles en el *Fausto* de GOETHE. Por la lógica bivalente, tantas veces denostada y sin embargo es la bivalencia donde colapsa el momento último de cualquier decisión humana[32]. Consideramos dicho estudio una buena introducción a la *abstracción*; abre nuestras mentes y genera esquemas de pensamiento insospechados. El que las *paradojas* —perfectas ejemplificadoras de caminos argumentales no válidos—, lógicas, semánticas, puedan surgir en cualquier momento en el quehacer investigador es una buena fuente de quebraderos de cabeza. Sin embargo, la identificación de su origen y cómo evitarlas o reconducirlas, son objetivos muchas veces alcanzables.

Las *falacias*, esas seudoargumentaciones capciosas y torticeras que eternamente aquejan a la clase política[33], desdoro de ella, en su incesante demagogia, en su celo por la posverdad, en su permanente desamparo y desmedro de la dialéctica en favor de una burda retórica plagada de aderezos prescindibles, incoherente oratoria e infame panegírica, en su constante juego de disfraces de me-

[31] Aunque no esté de más contar con ellas en ciertos entornos —«Y cuando la guerra haya terminado, algún día, los libros podrán ser escritos de nuevo. La gente será convocada una por una, para que recite lo que sabe, y lo imprimiremos hasta que llegue otra Era de Oscuridad, en la que, quizá, debamos repetir toda la operación» (*cfr. Farenheit 451*, de Ray BRADBURY)—; en la misma ronda nos encontramos con los Libros Humanos (https://humanlibrary.org/meet-our-human-books/) de la *Human Library Organisation* (HLO) (https://humanlibrary.org/) —las Bibliotecas Humanas son acaecimientos interactivos que brindan la oportunidad de conocer a alguien que de otra manera nunca habríamos conocido, seguramente debido a su origen o entorno; somos quienes «leemos», tomando «prestada» una persona con experiencia en prejuicios, estereotipos y discriminación, un «libro humano» cuya historia escucharemos, a quien preguntaremos, con quien conversaremos y contrastaremos nuestras propias ideas, experiencia y puntos de vista, propiciándose la génesis de una revisión de lo particular, depurada, sintética, asequible y atractiva, pudiéndose sacar a la luz, divulgarse, para que fructifique, lo académico en lo social, y viceversa, pura CTS—.

[32] ¿Qué uso de razón prefiere la ambivalencia?

[33] *Cfr. v. gr.* RUBIALES [12] y SIERRA FRANCO [13] (págs. 49ss.).

táforas y eufemismos encubridores de inverosimilitudes, de sutiles simplificaciones y distorsiones, espurias aquéllas y genuinas éstas, de sugerentes y populistas epítomes, todos artificios efímeros que afloran por doquier y salen a luz cuando se desarrebozan sus entramados subrepticios; las falacias, sofismas y paralogismos constituyen otra de tantas cuestiones sobre las que las personas deberíamos estar alerta, a un tiempo y andando el tiempo[34], mayormente por si también nosotras mismas incurrimos en estas mentiras sin impostura alguna y para que subsiga el ejercitarnos en la frustación de la reincidencia. Y en el mientras, la susodicha clase, acogedora y promotora sin vergüenza de la indigencia mental, pervive abandonada a su cerrilidad en la exigencia constante de que sus ocurrencias se impongan con rango de norma. Lo peor, lo mismo. El juego de danza entre las apariencias y el relativismo: un trabajo indecente de gran calado. Por Dios, que sin dialéctica no hay progreso científico[35]; ¡contumacia en su porfía!

Pero tampoco se salvan de ellas los acaecimientos presentes y pasados, la historia [36].

La práctica de la *construcción, reconstrucción, ratificación y corroboración de argumentos* se postulan como piezas claves para el análisis lógico de los mismos, para su *formalización* y *resolución* —ya *convalidación*, ya *invalidación*—, y, por ende, en beneficio de nuestra pericia en la comprensión y análisis crítico de textos, discursos y relatos. Cual alegato de la memoria, la escritura y la retórica.

Ni existe una única lógica, ni una es mejor que otra. El desarrollo de unas y otras quizás avance por modas y tanto aquél como su finalidad dependen de entornos, tendencias o estados de opinión consolidados (convencionalismos colectivos), a veces, por inmovilismo consecuencia del agotamiento de «pensamientos» no críticos, y otras, por meras comensalías académicas. Cada concepción de la lógica, cada cimentación, conduce analíticamente a sus propias conclusiones y soluciones. A pesar de no ser más que meras colecciones de herramientas, desde la perspectiva humana, o sea, aparentemente, el pensamiento sistemático que suponen favorece sin duda el desarrollo de las humanidades, la ciencia, la tecnología y la sociedad.

Haciendo mochila con la lógica, a su arrullo, iniciamos la andadura del resto de capítulos con paso firme por el camino del rigor en el *lenguaje lógico-matemático*. Es opinión de quien escribe que deberíamos prestar atención en todo momento a realizar la *traducción* de éste a nuestra lengua materna y cómo hacer la *traducción inversa*, desde nuestra lengua materna al lenguaje lógico-matemático —cuidado en ambos sentidos, humanamente *traducir demanda comprender*— y que deberíamos ejercitarnos constantemente en ello porque tener la capacidad de traducir en ambos sentidos y convertirnos en ambilingües es menester insoslayable para pensar y hablar las matemáticas y para ser conscientes no sólo de lo que aprendemos sino también de cómo lo aprendemos, porque, en definitiva, es un requisito ineludible para *comprender, componer y extender las matemáticas*.[37]

[34] *Duo si idem dicunt non est idem* (José Ortega y Gasset, «Prólogo para franceses», *La rebelión de las masas*, 1937).
[35] *Cfr. v. gr.* Rescher [14].
[36] *Cfr. v. gr.* Tarín Alonso [15].
[37] ¿Quién será quien verifique lo traducido? A tener presente: el vocabulario seleccionado por cada persona, el significado de cada palabra en boca de cada persona, y las reglas sociales de interacción verbal entre las personas. De nuevo, el alegato de Ortega[34] , al que respondemos: *communi consensu*.

Si bien el talento está presente en la metodología, en la planificación, ejecución y verificación del qué y del cómo, en mucha mayor medida lo está el esfuerzo, el instinto, la emoción, el alma. Además, lo que del primero se sufre, lo segundo lo calma.

Y el *error*, adversidad a la vez que dicha. Jean Pierre Astolfi [16] considera éste un medio para enseñar; Elena Sanz [17] destaca cómo diversos estudios parecen indicar que impulsa un aprendizaje imposible sin él; más allá aún, pienso en él como un engranaje clave para la enseñanza y el (auto)aprendizaje (auto)correctivo; hemos de hacer hincapié en ellos, pues tras el error, mediante la *retroalimentación*, se aprende de él y, particularmente, a cómo evitarlo en el futuro, redescubriéndonos, reiventándonos, adaptándonos, resurgiendo; estoy convencido de que el error puede promover la *indagación*, la *creación*, el *perfeccionamiento*.

Error, porque el fracaso, la derrota, no existe. O lo logras, o aprendes, no más.[38]

Entremedias y entretejida, la *práctica*, o mejor, el apego a ella, con empeño, sin límites; habilitadora del dominio de la técnica, la elegancia y la precisión, procedamos con la práctica con constancia, ritmo y contención. Las cuestiones resueltas o propuestas, en su mayoría ejemplos, ejercicios y problemas, desde instrumentales a mayor complejidad, forman parte del acervo popular de entrenamiento matemático, recogidos en varios textos, a alguno de los cuales, siempre que me ha sido posible, he hecho referencia[39].

Dicho lo cual, así como por otra parte y en cualquier caso, los *esquemas de resolución* que proporciono lo son a modo de sugerencia de respuestas, sin ánimo de pronunciamiento docto ni concluyente alguno. Quedaré muy agradecido a aquellas personas que me hagan saber de errores que detecten en ellos o en el resto de las NIC.

Tengo la seguridad de que ninguna persona sensata y mucho menos cabal piensa que pudiese dominar una materia científica sólo asistiendo a clases y leyendo libros de textos, artículos o ensayos. Dedicar tiempo a la práctica es imprescindible. Únicamente con la práctica adquirimos una correcta percepción de lo factible en cada situación. Con la práctica repetitiva, para afianzar lo aprendido. Con la práctica reflexiva, conociendo el porqué va a fracasar o triunfar una estrategia determinada en una realidad concreta. Práctica basada en la resolución, en la búsqueda de soluciones, no en memorizar éstas.[40]

[38] «¿Que es ello absurdo, decís? ¿Y quién sabe qué es lo absurdo? ¡Y aunque lo fuera! Solo el que ensaya lo absurdo es capaz de conquistar lo imposible. No hay más que un modo de dar una vez en el clavo, y es dar ciento en la herradura. Y, sobre todo, no hay más que un modo de triunfar de veras: arrostrar el ridículo.» (Miguel de Unamuno y Jugo , *Vida de Don Quijote y Sancho*, 1958, Capítulo XLV: Donde se acaba de averiguar la duda del yelmo de Mambrino y de la albarda, y otras aventuras sucedidas con toda verdad: https://www.cervantesvirtual.com/obra/vida-de-don-quijote-y-sancho-785968/).

[39] He hecho los imposibles para asegurar no haber infringido *derechos de autoría* de terceros al publicar estas cuestiones, ya de hecho en la memoria colectiva matemática. Agradezco cualquier información que pudiese ayudarme a hacer un reconocimiento de autoría correcto. Nada más conocerla, la publicaré apropiadamente.

[40] «Una vez que hayas asimilado lo que aquí te he escrito, podrás resolver infinitud de problemas que yo no te he planteado en mi escrito, ya que te habré proporcionado una vía para solucionar la mayoría de tales problemas al haberte descrito un ejemplo de cada especie» (Diofanto, *Aritméticas*, IV, Introducción; vía Houlou-Garcia [18]).

La práctica y su análisis son esenciales para acrecentar nuestro conocimiento y engrosar nuestra memoria, para superar los juicios que nos limitan y multiplicar nuestra motivación a través de la manifestación de lo tangible, contribuyendo a la inevitabilidad de nuestro éxito. Cuando practicamos, tenemos en mente un objetivo claro, aunque sea el simple hecho de encontrar la solución, la respuesta a lo cuestionado.

Lo cual, sin duda, demanda una pausa que permita una pequeña exploración.

Una exploración de la información presente y del conocimiento del pasado. Porque con la práctica, resolveremos cuestiones nuevas mediante su identificación a través del conocimiento con modelos matemáticos y esquemas algorítmicos conocidos en virtud de la memoria, modelos y esquemas, a modo de bases —prototipos—, estudiados y memorizados, aún quizás esto último sin ser conscientes de ello.

Por la necesidad de la práctica, no es el estudio de los métodos en sí el único objeto, sin embargo, el conocimiento teórico —a veces confundido como constructo histórico con el sentido común— y las relaciones, no sólo teóricas, también conceptuales y empíricas, que lo entreveran y lo ligan a la praxis, son esenciales para mostrar, debatir y crear, y para cuestionar —sobre todo, para cuestionar— lo inferido y dado por concluso, estremeciendo, si no incluso renovando, los mismos cimientos.

Mas hemos de tener cuidado, si bien el conocimiento media en la identificación, también lo hace la intuición. Razonar y formar, comparativamente, por analogía, es intuitivo y, por tanto, arriesgado[41].

Decálogo:

0.º, cierto es que no solemos aprender en fecha fija, sino cuando lo necesitamos para resolver un problema o gestionar una situación, sin embargo, creo que el siguiente decálogo puede sernos de ayuda;

1.º, estudiemos la ruta para saber lo que hay que hacer, hagámonos con toda la información posible;

2.º, planifiquemos la marcha —la ruta es larga—, horas inicial y final diarias, teniendo en cuenta descansos e imprevistos;

3.º, seamos previsores, recordemos cómo nos ha ido en jornadas anteriores para hacernos una idea del esfuerzo que supone una sesión de estudio;

[41] «La intuición es la inteligencia del inconsciente» (Carl Gustav Jung). En mi caso, la considero esencial para poder andar nuevos caminos, y recomiendo atenderla. No sé si en relación, pero me viene a la memoria aquello que cuentan acerca de George Dantzig y su resolución de aquella pareja de problemas abiertos que dicen que confundió con tareas de clase (*vid. v. gr.* https://es.wikipedia.org/wiki/George_Dantzig), anécdota que inspiró la película *El indomable Will Hunting* (*vid. v. gr.* https://www.xataka.com/investigacion/el-indomable-george-dantzig-y-la-verdad-que-esconden-las-leyendas-urbanas), y a mí la propuesta de las cuestiones A.37 y A.38 (págs. 1437 y 1437, respectivamente, de esta edición) en los exámenes p.h.e.c. en el año del confinamiento por covid.

4.º, equipémonos, adaptemos la cantidad de recursos y materiales de estudio —apuntes, libros, multimedia, etc. (nuestra caja de herramientas)— según la duración estimada y la previsión realizada;

5.º, «calentemos», empecemos repasando lo estudiado en días anteriores;

6.º, comencemos con poca bibliografía, por ejemplo los apuntes, después, según la intensidad del estudio, incorporaremos más capas bibliográficas;

7.º, sigamos un ritmo, comencemos con un vistazo general, lentamente para aumentar progresivamente el ritmo, evitando los cambios bruscos, hasta alcanzar una cadencia constante;

8.º, descansemos regularmente, sobre todo si el horario de estudio para ese día es extenso (examen cercano, por ejemplo);

9.º, elijamos una técnica adecuada, cuanto más difícil el contenido, más despacio, no saltemos ni demos por hecho nada, y

10.º, adaptémonos, seamos flexibles ante cambios o situaciones inesperadas.

Porque, la matemática es una actividad, —insistamos— de planificación, traza y recorrido de un camino personal, y esto requiere un aprendizaje no rutinario, consciente, crítico y reflexivo, cuestionando los presupuestos, discutiendo los argumentos, cometiendo errores, teniendo dudas permanentemente, y creando nuevos escenarios reales o posibles y mundos imaginarios.

No existe mejor estímulo que disfrutar de la esencia de lo aprendido para luchar por su conservación, sean las ciencias, en particular, la matemática, las humanidades —tan denostadas éstas por la clase política, pero fundamentales para este pensamiento crítico demandado—, en particular, la filosofía, o la propia naturaleza. Somos conscientes de esto: quien se queda en la superficie jamás será partícipe de los tesoros ocultos en las profundidades.[42]

[42] «Para la persona religiosa, Dios se da de manera directa e inmediata. Él y su voluntad omnipotente son la fuente de toda vida y de todos los acontecimientos, tanto en el mundo mundano como en el mundo del espíritu. Aunque no puede ser comprendido por la razón, los símbolos religiosos ofrecen una visión directa de Él, y Él planta su santo mensaje en las almas de aquellos que se confían fielmente a Él. En contraste con esto, el científico natural no reconoce como algo dado de forma inmediata más que el contenido de sus experiencias sensoriales y de las mediciones basadas en ellas. Partiendo de este punto, emprende un camino de investigación inductiva para acercarse lo mejor posible a la meta suprema y eternamente inalcanzable de su búsqueda: Dios y Su orden mundial. Por lo tanto, aunque tanto la religión como la ciencia natural requieren la creencia en Dios para sus actividades, para la primera Él es el punto de partida, para la segunda la meta de todo proceso de pensamiento. Para la primera Él es el fundamento, para la segunda la corona del edificio de toda cosmovisión generalizada. […] No importa dónde y cuán lejos miremos, en ninguna parte encontramos una contradicción entre la religión y las ciencias naturales. Por el contrario, encontramos una concordancia completa en los puntos de importancia decisiva. La religión y las ciencias naturales no se excluyen mutuamente, como muchos de nuestros contemporáneos creen o temen; se complementan y condicionan mutuamente. La prueba más inmediata de la compatibilidad entre la religión y las ciencias naturales, incluso bajo el escrutinio crítico más minucioso, es el hecho histórico de que los científicos naturales más grandes de todos los tiempos —hombres como Kepler, Newton, Leibniz— estaban impregnados de una actitud religiosa muy profunda. […] La religión y la ciencia natural libran una batalla conjunta en una cruzada incesante y sin tregua contra el escepticismo y el dogmatismo, contra la incredulidad y la superstición, y el grito de guerra en esta cruzada siempre ha sido, y siempre será: "¡Hacia Dios!"» (*To the religious person, God is directly and immediately*

Demostración de una cuestión

Para *demostrar una cuestión*, sean éstas o cualquier otra, en general, debiésemos:

I. *analizar* la cuestión, esto es, estudiémosla hasta obtener una idea clara y concisa, es decir, que con nuestras propias palabras sepamos explicarla y sepamos qué teoría lógico-matemática vamos a necesitar para su resolución;
II. *diseñar* la resolución, esto es, indiquemos los pasos a seguir para resolverla;
III. *codificar* la resolución, esto es, a medida que desarrollamos los pasos que hemos determinado, utilicemos correctamente el lenguaje lógico-matemático;
IV. *interpretar* la solución obtenida y *evaluar* su consistencia con el enunciado y la solución perseguida;
V. *documentar* la resolución de manera que pueda ser entendida por parte de otra persona, incuida por la nuestra pasado un tiempo;
VI. *hacer* la demostración por diferentes vías, estrategias, métodos, técnicas.

Recordémoslo siempre: sin conocimiento no hay pensamiento crítico. Así que debemos salvaguardar nuestro conocimiento. Debemos *asentar nuestro aprendizaje*, hemos de encontrar una estrategia de documentación y registro, interno —como un palacio de la memoria[43]— y externo —como un cuaderno de bitácora vital, un diario de vida—, en previsión de futuras ocasiones en las que necesitemos lo aprendido, considerando siempre los valores humanos en Ciencia, Tecnología y Sociedad[44] (CTS), entre otros: fuerza de voluntad, superación y personalidad; curiosidad, esfuerzo y trabajo; estudio, respeto y responsabilidad; escucha activa, paciencia y empatía; generosidad, honestidad y sinceridad; compromiso, constancia y lealtad; solidaridad, trabajo en equipo, corrección y nobleza; amor, justicia y libertad.

> Los problemas que desaparecen por sí mismos vuelven por sí mismos.
>
> (Paul Dickson (1980), *The Official Explanations*).

given. He and His omnipotent Will are the fountainhead of all life and all happenings, both in the mundane world and in the world of the spirit. Even though He cannot be grasped by reason, the religious symbols give a direct view of Him, and He plants His holy message in the souls of those who faithfully entrust themselves to Him. In contrast to this, the natural scientist recognizes as immediately given nothing but the content of his sense experiences and of the measurements based on them. He starts out from this point, on a road of inductive research, to approach as best he can the supreme and eternally unattainable goal of his quest—God and His world order. Therefore, while both religion and natural science require a belief in God for their activities, to the former He is the starting point, to the latter the goal of every thought process. To the former He is the foundation, to the latter the crown of the edifice of every generalized world view. […] No matter where and how far we look, nowhere do we find a contradiction between religion and natural science. On the contrary, we find a complete concordance in the very points of decisive importance. Religion and natural science do not exclude each other, as many contemporaries of ours would believe or fear; they mutually supplement and condition each other. The most immediate proof of the compatibility of religion and natural science, even under the most thorough critical scrutiny, is the historic fact that the very greatest natural scientists of all times—men such as Kepler, Newton, Leibniz—were permeated by a most profound religious attitude. […] Religion and natural science are fighting a joint battle in an incessant, never relaxing crusade against scepticism and against dogmatism, against disbelief and against superstition, and the rallying cry in this crusade has always been, and always will be: “On to God!””) (Max Planck, *Religion und Naturwissenschaft*, una conferencia, impartida en mayo de 1937 [versión en inglés procedente de *Scientific Autobiography And Other Papers*, 1950, págs. 151–187: https://archive.org/details/in.ernet.dli.2015.177537]).

[43] *Vid. v. gr.* https://en.wikipedia.org/wiki/Method_of_loci.

[44] *Vid. v. gr.* https://es.wikipedia.org/wiki/Estudios_de_ciencia,_tecnología_y_sociedad.

Leamos, estudiemos, preguntemos,
profundicemos, contrastemos, reflexionemos,
debatamos, entrenemos, enseñemos,
hilvanemos, interioricemos,
que brote nuestra curiosidad insaciable,
resolvamos ejercicios,
reescribamos demostraciones y ejemplos,
busquemos éstos, negativos y positivos,
tratemos de explicarlos
en términos de conceptos fundamentales,
y también de descubrir
nuevas formas de demostrar lo propuesto,
tranquilidad,
no todo se comprende de primeras,
releamos, repensemos,
papel, lápiz y paciencia,
así, y sólo así,
podremos finalmente enfrentarnos
a la resolución de nuevas situaciones,
y «robar»[45] la matemática.
No prosigamos hasta ser conscientes y firmes.
Impidamos la entrada a la procrastinación y al abotargamiento.

¿Para qué llamar caminos
a los surcos del azar?…
Todo el que camina anda,
como Jesús, sobre el mar.

(Antonio Machado, *Campos de Castilla*, Proverbios y Cantares, II).

[45] Me refiero a la aplicación de la matemática en la vida ordinaria; la metáfora es de Raúl Ibáñez Torres [19].

La historia enseña
que la desigualdad social proviene
de la desigualdad cultural
y ésta de la desigualdad en la educación.

Una sociedad desinformada
y, en particular, científicamente ignorante
(el ideal de algunas personas ocupantes de la política),
es incapaz de intervenir conscientemente
en la toma de decisiones de calado
y de discriminar entre lo seudocientífico
y la verdadera ciencia.

Compartamos conocimiento
con las menos trabas posibles,
o sin ninguna.

Compartamos conocimiento
colaborando en su construcción,
sin atesorar lo que sabemos,
y no sólo en los quehaceres discente y docente
ni únicamente en lo que se refiera a unos saberes concretos,
sino en todo y siempre.

Esto debería enseñarse desde la infancia[46].

Promovamos el valor de colaborar, cooperar y compartir,
mas sin esperar recompensa alguna.
Fomentémoslo incluso en los exámenes,
cuyo valor formativo alcanzaría todo su esplendor.

El conocimiento libre[47], abierto y gratuito
es un pilar fundamental para combatir
la propagación de la ignorancia,
el oscurantismo
y la estulticia
en la sociedad.

Cambiemos la realidad social.

[46] «Educar desde la raíz para cambiar el mundo. Educar es urgente y lo tenemos que hacer hoy para garantizar un mañana que no deje a nadie atrás. Porque el mundo tiene mucho que sanar, pero sobre todo mucho que aprender» (Educo, https://www.educo.org/).

[47] *Vid. v. gr.* https://es.wikipedia.org/wiki/Conocimiento_libre. Las ventajas del conocimiento libre son varias: desde la económica (la no necesidad de pagar regalías, si bien pudiese pagarse por mantenimiento o servicios) hasta la enseñanza de los valores subyacentes a lo libre, pasando por el inestimable valor de una fuente abierta, de poder conocer algo hasta lo más profundo, sin ningún cierre ni impedimento. ¿Inconvenientes? Quizás no debiésemos olvidar la realidad social, la cual, en estos momentos, usa ampliamente de forma no libre el conocimiento, lo usa tal cual mercancía. Sin embargo, esto no debiese impedir continuar con la enseñanza y el uso de lo libre, sino al contrario, porque cuanto más nos esforcemos, dentro y fuera del ámbito educativo, más probabilidad habrá de conseguir hacer de su uso mayoritario una realidad social en la que se comparta conocimiento con las menos trabas posibles, o mejor, sin ninguna, en la que lo compartamos colaborando en su construcción, sin guardarnos nada de lo que sepamos que pueda hacerse público, y todo esto, gratuitamente, sin esperar recompensa alguna. (Cooperar no es dar lo que nos sobra, cooperamos cuando damos parte nuestra, porque si nos sobra igual pudiésemos haberlo tirado a la basura).

¡Ojalá vinieseis todos henchidos de frescura, sin la huella que os han dejado quince o veinte exámenes, y trayendo a estos claustros no ansia de notas sino sed de verdad y anhelo de saber para la vida, y con ellos aire de la plaza, del campo, del pueblo, de la gran escuela de la vida espontánea y libre!

(Miguel de UNAMUNO Y JUGO , Discurso leído en la solemne apertura del curso académico de 1900 a 1901 en la Universidad de Salamanca (ordenado y dispuesto para la imprenta por Adolfo Sotelo Vázquez), *Analecta Malacitana*, Vol. XXI, 1998, págs. 257-272: http://www.anmal.uma.es/Numero9/Discurso_Unamuno_II.htm).

El programa docente perfecto

¿Existe el programa docente cerrado perfecto? No. Se trata de una realidad variable que alumnado y profesorado descubre y ajusta en el día a día, aprendiendo y enseñando, aportándose mutuamente experiencia y conocimiento, tratando de realizar un trabajo realista, huyendo de especulaciones alejadas de la realidad y del conformismo y fatalismo que supondría la renuncia a mejorar lo existente. En sí, un programa docente no deja de ser una panoplia de ideas fundadas y buenas intenciones cuya realización está sujeta a la lealtad en el ejercicio y a la interpretación recta del, aún inédito, *código de práctica ética*.

Con todo esto en mente, recomiendo el desarrollo dinámico de la materia, a partir de una programación inicial, dúctil y abierta, no limitada por nada predeterminado, como debe ser para poder ser utilizada de manera flexible y creativa, permitiendo así a quienes la enseñen adaptarla para cumplir los objetivos del proceso de enseñanza (dinámico en su esencia) —teniendo presente no sólo su labor docente sino también su obligación de estudiar, investigar y transferir conocimiento a la sociedad—, una enseñanza basada en la evidencia, adaptada al ritmo al que quienes aprenden descubren y examinan ideas de manera autónoma, de forma que, de acuerdo a sus intereses particulares, puedan relacionar significativamente entre sí los diferentes conceptos estudiados con nuevos conocimientos encontrados, nuevas habilidades adquiridas o en desarrollo y nuevos caminos de exploración, surgidos de la práctica y experiencia.

No a las zonas de confort ni a las impuestas externamente. *Trabajar libremente, y en los márgenes*, cuanto más si limitan, es esencial para que éstos no se contraigan sino que se expandan. Esto permite y contribuye al autodescubrimiento, al crecimiento y al avance.

Que sí, que la ciencia y el conocimiento, en general, ni se busca ni se descubre ni se encuentra, se construye con voluntad y compromiso, en libertad.[48]

[48] *Cfr. v. gr.* León Rojas [20], [21], [22], [23], y las obras que refieren éstas.

Prefacio I: del lenguaje lógico-matemático

Verba volant, scripta manent.

(Cayo Tito).

Donde advertimos del uso de variantes del lenguaje lógico-matemático.

Estoy convencido de que en todo fenómeno empírico subyace un modelo lógico-matemático que permite su descripción y su interpretación humanística y científica. Que esto ocurra en toda concepción abstracta, aún es tema de discusión.

En cualquier caso, lo que parece indudable es que tanto para proponer tal modelo como para entender, hacer y comunicar matemáticas es necesario conocer el lenguaje lógico-matemático. Éste se manifiesta al menos en tres grados principales que incluso pudiésemos llamar variantes[49]:

0.ª, una puramente sintáctica, un juego de signos y símbolos, dado un contexto y unas reglas de juego determinados, con diferentes grados de rigor, a veces usando abreviaturas para facilitar dicho juego sintáctico; por ejemplo, las tres expresiones

- $(\forall x)(\forall y, z)(\langle x, y\rangle \wedge \langle x, z\rangle \to (\forall F\,(Fy \leftrightarrow Fz)))$,
- $(\forall x)(\forall y, z)(\langle x, y\rangle \wedge \langle x, z\rangle \to y = z)$,
- $(\forall x)(\exists! y)(\langle x, y\rangle)$,

son (meta)lógicamente equivalentes;

1.ª, una en la que incluimos una interpretación concreta del contexto, en este caso nuestro conocimiento de X, Y, R y F y de su naturaleza, por ejemplo, las mismas expresiones anteriores:

- $(\forall x \in X \subseteq \mathcal{U})(\forall y, z \in Y \subseteq \mathcal{U})$
  $(((\langle x, y\rangle \in R \subseteq X \times Y) \wedge (\langle x, z\rangle \in R \subseteq X \times Y) \to ((\forall F \in \mathrm{Pred})\,(Fy \leftrightarrow Fz)))$,
- $(\forall x \in X \subseteq \mathcal{U})(\forall y, z \in Y \subseteq \mathcal{U})$
  $((((\langle x, y\rangle \in R \subseteq X \times Y) \wedge (\langle x, z\rangle \in R \subseteq X \times Y)) \to y = z)$,
- $(\forall x \in X \subseteq \mathcal{U})(\exists! y \in Y \subseteq \mathcal{U})(\langle x, y\rangle \in R \subseteq X \times Y)$;

[49] Con cierto paralelismo al ámbito de la computación, pudiésemos decir de la 0.ª y la 1.ª que son dos formas de *código lógico-matemático* y de la 2.ª que es una forma de *pseudocódigo lógico-matemático*.

2.ª, una más natural, más próxima a nuestra lengua ordinaria, también en diferentes grados, por ejemplo, la última expresión anterior:

- para cualquier $x \in X$ existe como mucho un $y \in Y$ tal que $\langle x, y \rangle \in R$;
- para cualquier x de X existe como mucho un y en Y tal que x está relacionado con y por R;
- para cualquier elemento x del conjunto de nombre X existe como mucho un elemento y en el conjunto de nombre Y tal que x está relacionado con y por la relación diádica de nombre R;
- dado un referencial de nombre $\mathcal{U}$, para cualquier elemento x del conjunto de nombre X (que, como sabemos, es un subconjunto del referencial de nombre $\mathcal{U}$) existe un único elemento y en el conjunto de nombre Y (que, como sabemos, es un subconjunto del referencial de nombre $\mathcal{U}$) tal que x está relacionado con y por la relación diádica de nombre R (que, como sabemos, es un subconjunto del producto cartesiano de los conjuntos de nombre X e Y).

En nuestro estudio emplearemos las tres variantes, en sus diferentes grados, dependiendo del contexto.

Resta advertir que en estas notas, siempre que no se trate de lenguaje lógico-matemático y dado el significado concreto en dicho lenguaje de determinadas palabras y expresiones, nos referimos a un agregado de objetos como una *colección de entidades*:

- *colección* en vez de acervo, agregación, agregado, agrupación, clase, conglomerado, conjunto, cúmulo, familia, grupo, montón, pluralidad, reunión;
- *entidad*, por englobar a colectividades, en vez de elemento, ente, individuo, objeto, unidad.

Prefacio II: de la definición

Como es el pan será la sopa.

(Refrán).

Donde se intenta aclarar el concepto de definición, sus componentes, tipos y utilización.

El concepto de definición, entendida como la totalidad de atributos que caracterizan una colección determinada de entidades, tiene su origen en ARISTÓTELES. En toda definición se distingue entre lo definido (*definiendum*) y la expresión que lo define, el definiente (*definiens*). Los términos definientes, como delimitadores y, por tanto, determinadores, ya sea con funcionalidad de explicación (*definición explicativa o analítica*) o de conveniencia (*definición regulativa o sintética*), en cualquier caso deben ser inequívocos y preexistentes a la definición, bien porque hayan sido definidos ellos mismos con anterioridad por otros definientes, bien por haber sido admitidos como primitivas del sistema. Además, la definición debe ser consistente internamente, en sí misma, y con el sistema donde se realiza.

En una definición explicativa, caso particular de explicación, el *definiendum* se corresponde con el *explanandum*, el objeto de la explicación, y el *definiens* con el *explanans*, lo aducido a título de explicación. Por ejemplo, la explicación de *explanandum* $4 + 1 = 6$ y *explanans* $+1$ denota a la función «siguiente entidad en el orden» y se trabaja en el conjunto de los números naturales pares no negativos ordenados por el orden habitual $\{0, 2, 4, 6, 8, \ldots\}$.

En el lenguaje lógico-matemático, es frecuente el uso de definiciones regulativas para introducir abreviaturas o signos que designen conceptos o palabras o complejos de signos mayores; en este caso, lo definiente (el *definiens*) es lo que hay que abreviar y lo definido (el *definiendum*), lo ya abreviado. Se distinguen dos tipos de definiciones regulativas, las explícitas y las implícitas.

En una *definición explícita*, definido y definiente están claramente separados por un signo especial, metalingüístico, un definidor o igualador semiótico. Si notamos D al *definiendum* y d al *definiens*, en los textos aparece

$$D = d\ \mathrm{Df},\ D = \mathrm{df}\ d,\ D \overset{=}{\mathrm{D}} d,\ D \underset{\mathrm{df}}{=} d,\ D \overset{\mathrm{df}}{=} d,\ D =_{\mathrm{Def}} d,\ D \triangleq d \text{ o } D := d,$$

para expresar explícitamente que D es «igual por definición a» (o simplemente, es) d, aunque en muchos encontraremos la simple igualdad $D = d$ como medio de su expresión implícita —una notación similar se emplea en el caso de la «equivalencia por definición», $D :\equiv d$, $D :\Leftrightarrow d$—. Por nuestra parte y por comodidad de quien lee, utilizaremos cuando se requiera:

- $D \fallingdotseq d$ (*D se define como d*)[50];
- $D := d$ (*D es igual a d, por definición*, esto es, como consecuencia de que $D \fallingdotseq d$);
- $D :\Leftrightarrow d$ (*D es equivalente a d por definición*, esto es, como consecuencia de que $D \fallingdotseq d$);
- $D :\Rightarrow d$ (*D implica d por definición*, esto es, como consecuencia de que $D \fallingdotseq d$).

Por ejemplo, la derivada de una función f en un punto $x_0 \in \mathbb{R}$,

$$f'(x_0) \fallingdotseq \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}.$$

En ocasiones, usaremos palabras; abusando del lenguaje utilizaremos «si, y sólo si,» o «precisamente si»; por ejemplo: decimos que $*$ es conmutativa en X si, y sólo si, $(\forall x, y \in X)\ (x * y = y * x)$.

En una *definición implícita*, el *definiendum* y el *definiens*, aunque distinguibles, son inseparables. Por ejemplo,

$$y = log_a x \fallingdotseq a^y = x,$$

para la que una definición explícita[51] pudiese ser

$$log_a \fallingdotseq \{\langle x, y \rangle : a^y = x\}.$$

Un caso particular de definición implícita, lo constituye la *definición inductiva o recursiva*. Son definiciones compuestas. En primer lugar se definen explícitamente uno o más casos y ulteriormente se definen casos posteriores supuesto conocidas las definiciones explícitas primeras o anteriores. Por ejemplo, la función potencia, $\forall a \in \mathbb{R} \setminus \{0\}, \forall n \in \mathbb{N}$,

$$a^n \fallingdotseq \begin{cases} 1 & \text{si } n = 0, \\ a^{n-1}a & \text{si } n > 0, \end{cases}$$

en la que apreciamos que primero se define explícitamente la potencia 0, esto es,

$$a^0 \fallingdotseq 1,$$

[50] Paul LORENZEN, *Einführung in die operative Logik und Mathematik [Introducción a la Lógica Operativa y las Matemáticas]*, Springer-Verlag, Berlín, 1955.

[51] La lógica de primer orden —*vid. infra* el capítulo 4 (pág. 364 de esta edición)— satisface el *teorema de definibilidad de* BETH, esto es, cualquier definición implícita formulada en el lenguaje de la lógica de primer orden, puede formularse en forma explícita, y recíprocamente.

y después, para $n > 0$, suponiendo que ya ha sido definida la potencia $n-1$, se define la potencia n explícitamente a partir de la $n-1$, o sea,

$$a^n \leftrightharpoons a^{n-1}a.$$

Frecuentemente, en ausencia de interés metalingüístico, metalógico o metamatemático explícito[52], se relaja la notación anterior y se expresan las definiciones por simples igualdades. Así hemos procedido y procederemos. Por ejemplo, la función característica de un conjunto, tal que así:

Sea $\mu_X : X \longrightarrow \{0,1\}$, definida $\forall x \in X$ por $\mu_X(x) = 0$, si $x \notin X$ y por $\mu_X(x) = 1$, si $x \in X$.

Aún más, se usa la definición para permitir la introducción de signos nuevos, disminuyendo la complejidad notacional; por ejemplo, es frecuente usar «$x \leq y$» (o, sinónimamente, «$x \leq y$») como abreviatura de «$x < y$ o $x = y$», cuestión que queda reflejada al ser escrita la definición del nuevo signo:

$$x \leq y \leftrightharpoons (x < y) \vee (x = y).$$

Es viable usar variadamente esta funcionalidad. Así, por ejemplo, es posible expresar con el igualador semiótico la formalización lógica de *proposiciones auténticas*[53] con variables o funciones proposicionales; por ejemplo,

$$p \leftrightharpoons \text{Piedra movediza, moho no cobija,}$$
$$Px \leftrightharpoons x \text{ es un número primo,}$$

y también la de constantes, por ejemplo,

$$a \leftrightharpoons \text{añil,}$$

si bien, en muchos textos, ya aparece el signo $=$, ya dos puntos (:), ya nada, como igualador semiótico y, a veces, la constante o proposición, entrecomillada.

En otras ocasiones pudiésemos utilizar, bien el signo $\mapsto$ para resaltar la *traducción* que se realiza desde las constantes, variables o funciones proposicionales a las proposiciones auténticas, enunciadas en lenguaje ordinario, bien el signo $\leftarrow$ para resaltar la *traducción inversa*, desde las proposiciones

[52] Meta-lingüístico/lógico/matemático con el sentido de hablar acerca del lenguaje, de la lógica o de la matemática.
[53] *Vid. infra* § 0.4.1 (pág. 32 de esta edición).

auténticas a las constantes, variables o funciones proposicionales[54]; por ejemplo,

$$a \mapsto \text{MARÍA},$$
$$a \leftarrow\!\shortmid \text{MARÍA},$$
$$p \mapsto \text{A la cama no te irás sin saber una cosa más},$$
$$p \leftarrow\!\shortmid \text{A la cama no te irás sin saber una cosa más},$$
$$Px \mapsto x \text{ es un número par},$$
$$Px \leftarrow\!\shortmid x \text{ es un número par}.$$

[54] Las proposiciones auténticas están enunciadas en lenguaje ordinario, en nuestro caso, nuestra lengua materna, el español (L0). Las constantes, variables y funciones proposicionales están formuladas en lenguaje lógico-matemático (L1). La traducción se refiere a ir de los aductos en lenguaje lógico-matemático a nuestra lengua materna (de L1 a L0; por ejemplo, a traducir ∃ como «existe») y la traducción inversa a que nuestros eductos en lenguaje lógico-matemático correspondan fehacientemente a lo afirmado en nuestra lengua materna (de L0 a L1; por ejemplo, a que si escribimos ∃, sea porque es la traducción de «existe»).

Prefacio III: de ciertos preliminares

Cuando reanudamos la marcha, la noche caía, y como Paco pensara y pusiera por obra que "quien caminando lleva priesa, en camino llano tropieza", ya había cerrado con foscas nubes, cuando llegamos a Argamasilla de Alba, donde lo primero y último que vimos, paseando por la plaza, fue el triunvirato del médico titular, el bachiller Angel Pereyra (con y) y el licenciado Gómez.

(Augusto D'HALMAR, *La Mancha de Don Quijote*. En: *Obras escogidas*. Editorial Andrés Bello. Santiago de Chile, Región Metropolitana de Santiago (CL-RM), Chile, 1970, pág. 704).

Donde proporcionamos un sucinto *esquema* que contiene algunas *notaciones, ideas y enunciaciones iniciales* de las que aparecen en estas notas. De la 0 a la 6 se estudian por extenso en la parte dedicada a la cimentación. Nos concedemos la prerrogativa de marchar directamente al capítulo cero o al que nos interese en particular o volver aquí siempre que lo consideremos necesario, en definitiva, tanto *ex ante* (desde antes), *in itinere* (en camino) y *ex post* (desde después).

§ 0 De la lógica

Grosso modo, una proposición (simple) $p, q, r, \ldots$, es una oración declarativa de la que puede afirmarse sin lugar a dudas que es verdadera o falsa[55] pero no ambas cosas a la vez. Estas letras $p, q, r, \ldots$, con las que designamos las proposiciones, se llaman variables proposicionales. La negación de p (no p; $\neg p$) es la proposición que es verdadera si p es falsa y, recíprocamente, falsa si p es verdadera, en otras palabras, p es verdadera si, y sólo si, no p es falsa. La disyunción de p y q (p o q o ambas; $p \vee q$) es falsa si, y sólo si, lo son p y q. La conjunción de p y q (p y q; $p \wedge q$) es verdadera si, y sólo si, lo son p y q. La contravalencia de p y q (o bien p o bien q pero no ambas; $p \veebar q$) es falsa si, y sólo si, p y q son ambas falsas o ambas verdaderas. Decimos que p implica q es verdadera (si p, entonces q; $p \to q$) si, y sólo si, q es verdadera siempre que lo sea p; decimos, entonces, que p es condición suficiente para q y que q es condición necesaria para p. Decimos que p y q son equivalentes (p si, y sólo si, q; $p \leftrightarrow q$) si, y sólo si, p implica q y q implica p. Estas expresiones $\neg p$, $p \wedge q$, $p \to q$, $p \leftrightarrow q$, en el lenguaje de la lógica, son ejemplos de fórmulas o formas lógicas correspondientes a composición de proposiciones simples; $\neg(p \to (q \to q) \leftrightarrow (p \vee q))$ también es un ejemplo.

Enmarcadas en un universo de entidades $x, y, z, \ldots$: 0.°, la expresión $\forall x p(x)$ significa que para todo x se satisface la propiedad p (se trata del cuantor universal $\forall$); 1.°, la expresión $\exists x p(x)$ significa que la propiedad p es satisfecha por al menos una x (se trata del cuantor existencial $\exists$), y 2.°, la expresión $\exists! x p(x)$ significa que la propiedad p es satisfecha por una única entidad x (se trata del cuantor de existencia única $\exists!$). Hemos de tener cuidado con el anidamiento cuantorial y con las variables alcanzadas por cada cuantor; en general, $\forall x \exists y p(x, y)$, $\forall y \exists x p(x, y)$, $\exists x \forall y p(x, y)$ y $\exists y \forall x p(x, y)$ no son equivalentes.

§ 1 De los conjuntos, «ingenuamente»

Como noción primitiva entendemos por conjunto un agregado, una totalidad (vacía, finita o infinita) de entidades. Es claramente una definición vaga y, por tanto, no correcta, pero suficiente para comenzar nuestro trabajo. Algo más precisa es la definición de Cantor, un conjunto es la reunión en un todo de determinadas entidades bien definidas y diferenciables las unas de las otras. Decimos de cualquiera de ellas que es un elemento (o, sinónimamente, miembro) del conjunto y que está o pertenece a él. En la teoría «ingenua» de conjuntos, éstos suelen notarse con letras mayúsculas del alfabeto y sus elementos con minúsculas. En estas notas comenzaremos designándolos con minúscu-

[55] En el fondo, si bien con matices particulares de uso, se trata de una afirmación, afirmativa, aserción, aserto, aseveración, atestiguación, atestiguamiento, declaración, deposición, enunciación, manifestación, testimonio, testificación, sentencia. Además debe tener una formulación correcta (esto es, debe estar enunciada en términos claros y precisos). Por otro lado, puede estar acompañada por una confirmación (aducción de pruebas) o incluso por una demostración (argumentación que hace patente e indiscutible la verdad de la proposición).

las, aunque a partir de un cierto momento los notaremos con mayúsculas. Hemos de estar centrados y pendientes del contexto.

La afirmación $x \in y$, escrita en lenguaje lógico-matemático, representa la afirmación «x es un elemento de y» (o, sinónimamente, «y contiene a x»). Escribiremos la negación de $x \in y$ por $x \notin y$. Mediante «$x \subseteq y$» entenderemos que todo elemento de x lo es también de y (y diremos que x está `incluido` en y o que x es un `subconjunto` de y) (o, sinónimamente, que y incluye a x o que y es un `superconjunto` de x, e independientemente usar la notación explícita «$y \supseteq x$» para ello). Notaremos que dos entidades u y v son iguales por $u = v$ y que son distintas por $u \neq v$. Diremos así que dos conjuntos son iguales, $x = y$ si, y sólo si, $x \subseteq y$ y $y \subseteq x$, esto es, precisamente si x e y tienen los mismos elementos ($x \subseteq y$: todo elemento de x lo es de y; $y \subseteq x$: todo elemento de y lo es de x). Decimos que un conjunto x es un `subconjunto propio` de un conjunto y y se escribimos $x \subset y$ (o $x \subsetneq y$ o $x \subsetneqq y$ o $x \underset{\neq}{\subseteq} y$), precisamente si $x \subseteq y$ y $x \neq y$.

Definimos nuevos conjuntos. Dado un conjunto x, su `conjunto potencia`, que notamos $\mathcal{P}(x)$ (o, sinónimamente, 2^x), es el conjunto de todos los subconjuntos de x. La `intersección` de x e y, que notamos $x \cap y$, es el conjunto de todas las entidades que son elementos de x e y a la vez. La `unión` de x e y, que notamos $x \cup y$, como el conjunto de todos los elementos de x o de y o de ambos. El `complemento relativo` $\complement_x(y)$ es el conjunto de elementos de x que no son de y. En cada situación concreta puede definirse un `conjunto universal` $\mathfrak{U}$ como el conjunto de todas las entidades que intervienen en la situación. El `complemento` de un conjunto x es el conjunto de entidades que no son elementos de x, esto es, $\complement_{\mathfrak{U}}(x)$, aunque lo notamos simplemente por $x^\complement$. El `conjunto diferencia` de x e y, que notamos $x \setminus y$ (o $x - y$), es el conjunto de entidades que son elementos de x y no lo son de y, esto es, el conjunto $x \cap y^\complement$. Postulamos la existencia del `conjunto vacío` $\emptyset$, un conjunto sin elementos. Si $x \cap y = \emptyset$, decimos que x e y son `conjuntos disjuntos`. Destacan varias propiedades, entre otras: $x \cap x = x$ (en particular, $x \cap \emptyset = \emptyset$), $x \cup x = x$ (en particular, $x \cup \emptyset = x$), $x \cap y = y \cap x$, $x \cup y = y \cup x$, $(x \cap y) \cap z = x \cap (y \cap z)$, $(x \cup y) \cup z = x \cup (y \cup z)$, $x \cap (y \cup z) = (x \cap y) \cup (x \cap z)$, $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$, $x \setminus x = \emptyset$, $x \setminus \emptyset = x$, $\emptyset \setminus x = \emptyset$, $\emptyset^\complement = \mathfrak{U}$, $\mathfrak{U}^\complement = \emptyset$, $(x \cap y)^\complement = x^\complement \cup y^\complement$, $(x \cup y)^\complement = x^\complement \cap y^\complement$, $(x^\complement)^\complement = x$.

§ 2 De las relaciones

Un conjunto $\{x, y\}$, con $x \neq y$, también se denomina `par no ordenado`. Adoptamos la definición de KURATOWSKI de `par ordenado` $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$. Llamamos `producto cartesiano` de X e Y y se nota $X \times Y$ al conjunto de todos los pares ordenados $\langle x, y\rangle$ tales que $x \in X$ e $y \in Y$. Si $X = Y$, $X \times Y$ lo notamos X^2. Observemos que si $x \neq y$, entonces $\{x, y\} = \{y, x\}$ pero $\langle x, y\rangle \neq \langle y, x\rangle$. Si $x = y$, se tienen, respectivamente, el `conjunto unitario` $\{x\}$ y la `tupla unitaria` (o, sinónimamente, `tupla monádica`) $\langle x\rangle$. Dos pares ordenados son iguales si, y sólo si, son iguales elemento ordenado a elemento ordenado, esto es, $\langle x, y\rangle = \langle u, v\rangle \leftrightarrow x = u \wedge y = v$. Ex-

tendemos el concepto de par ordenado como caso particular de tupla[56]; en particular, hablaremos de `tupla enádica` (o, sinónimamente, `enetupla` o `n-tupla`)[57] $\langle x_0, x_1, \ldots, x_{n-1}\rangle$, satisfaciéndose que $\langle x_0, x_1, \ldots, x_{n-1}\rangle = \langle y_0, y_1, \ldots, y_{n-1}\rangle \leftrightarrow x_0 = y_0, x_1 = y_1, \ldots, x_{n-1} = y_{n-1}$. Llamamos producto cartesiano de $X_0, X_1, \ldots, X_{n-2}$ y X_{n-1} y notamos $X_0 \times X_1 \times \ldots \times X_{n-1}$ al conjunto de todas las enetuplas $\langle x_0, x_1, \ldots, x_{n-1}\rangle$ tales que $x_0 \in X_0, x_1 \in X_1, \ldots, x_{n-1} \in X_{n-1}$. Si $X_0 = X_1 = \ldots = X_{n-1} = X$, $X_0 \times X_1 \times \ldots \times X_{n-1}$, lo notamos X^n.

Una `relación enádica` (o, sinónimamente, `relación n-ádica`, `relación enaria`, `relación n-aria` o `relación poliádica de n argumentos`) es un subconjunto de enetuplas de un producto cartesiano $X_0 \times X_1 \times \ldots \times X_{n-1}$. Si $n = 2$ la llamamos `relación diádica` (o, sinónimamente, `relación binaria`) (esto es, es un subconjunto de pares ordenados de un producto cartesiano de dos conjuntos). Si $X_0 = X_1 = \ldots = X_{n-1} = X$, la llamamos *relación enádica en* X y para el caso $n = 2$ la llamamos *relación diádica en* X (es decir, no es más que un subconjunto de pares ordenados de X^2) y para el caso $n = 1$, *propiedad del conjunto* X (o sea, es un subconjunto de X).

Sean I y A dos conjuntos; una `familia de elementos` de A con `conjunto de índices` I es una `relación funcional` de I en A con dominio I. Es habitual representar dicha relación funcional por $(a_i)_{i\in I}$. Dado un conjunto I, una `familia de conjuntos` con conjunto de índices I es una relación funcional con dominio I. Dado un conjunto A y un conjunto $I \neq \emptyset$, llamamos `familia de subconjuntos` de A con conjunto de índices I a toda relación funcional de I en 2^A con dominio I. Como para el caso de elementos se usan paréntesis, así es habitual representar esta relación funcional por $(A_i)_{i\in I}$ (observemos su vista como sucesión indizada).

Destacamos el hecho de que una relación pueda ser: una `relación de equivalencia` (reflexiva, simétrica y transitiva), una `relación de tolerancia` (reflexiva y simétrica), una `relación de orden parcial` (reflexiva, antisimétrica y transitiva) y una `relación de preferencia` (reflexiva y transitiva).

§ 3 De las funciones y aplicaciones

A una relación diádica cualquiera $f \subseteq X \times Y$ también la llamamos `correspondencia` de X en Y (o, sinónimamente, en X de valor o *valorada* en Y). Decimos que f es una `relación funcional` precisamente si es tal que para cualquier $x \in X$ existe como mucho un $y \in Y$ tal que $\langle x, y\rangle \in f$, esto es, $(\forall x \in X)(\forall y, z \in Y)(\langle x, y\rangle \in f \wedge \langle x, z\rangle \in f \rightarrow y = z)$. A una relación funcional también se la conoce como `función parcial` de X en Y. En este ámbito, en vez de escribir $f \subseteq X \times Y$ y $\langle x, y\rangle \in f$, escribimos $f\colon X \longrightarrow Y$ y $f(x) = y$, respectivamente. Así destacamos la posible dependencia de y

[56] Entendemos por tupla una hilera ordenada de entidades (*cfr. v. gr.* https://www.rae.es/dpd/tupla).

[57] Evitamos usar «nupla» ya que en ciertos lenguajes de programación este término indica una tupla cuyos elementos son accesibles por nombre en vez, o además, de por índice. Sí usaremos `tupla kádica`, o simplemente, `katupla`, en vez de k-tupla, y tupla emádica, o simplemente, `emetupla`, en vez de m-tupla.

(la `variable dependiente`) de x (la `variable independiente`). De una relación funcional tal que $\operatorname{dom} f = X$ (todo el conjunto origen) decimos que es una `función total` o `aplicación` de X en Y.

Dados X, Y, V, W conjuntos, con $Y \subseteq V$, y $f : X \longrightarrow Y$ y $g : V \longrightarrow W$ funciones tales que $\operatorname{im}(f) \subseteq \operatorname{dom}(g)$, la composición $g \circ f : X \longrightarrow W, x \longmapsto (g \circ f)(x) = g(f(x))$ es una función: la `función compuesta` de f y g.

§ 4 De las estructuras algebraicas

§ 4.0 Leyes de composición

Sean tres conjuntos no vacíos X, Y, Z. Una `ley de composición` es una aplicación de $X \times Y$ en Z, $\langle x, y\rangle \longmapsto z = f(x, y)$ (los elementos x e y se componen dando lugar a otro elemento z). Llamamos `ley de composición interna` (l.c.i.) u `operación` en X (o entre los elementos de X) a toda aplicación $*$ de $X \times X$ en X, $\langle x, y\rangle \longmapsto x * y$, llamando a $x * y$ la composición de x con y (el resultado de operar x con y). Lamamos `ley de composición externa` (l.c.e.) en X a toda aplicación $f : S \times X \longrightarrow X$, $\langle \alpha, x\rangle \longmapsto f(\alpha, x)$, siendo habitual notar $f(\alpha, x)$ simplemente por αx (suele denominarse `conjunto de escalares` a S).

Dada la l.c.i. $*$ en X, decimos que: 0.º, $*$ satisface la `propiedad conmutativa` (o, simplemente, que es conmutativa) en X si, y sólo si, $(\forall x, y \in X)\,(x * y = y * x)$; 1.º, $*$ satisface la `propiedad asociativa` en X si, y sólo si, $(\forall x, y, z \in X)\,((x * y) * z = x * (y * z))$; 2.º, X tiene `elemento neutro` respecto de $*$ si, y sólo si, $(\exists e \in X)(\forall x \in X)(e * x = x * e = x)$ (de existir el neutro, es único); 3.º, existe el `elemento simétrico` de $x \in X$ en X respecto de $*$ si, y sólo si, $*$ tiene elemento neutro e en X y $(\exists x' \in X)(x' * x = x * x' = e)$ (decimos que x' es el simétrico de x en X) (si $*$ es asociativa en X, de existir el simétrico de un elemento, es único), y 4.º, decimos que $x \in X$ es un `elemento simplificable` en X respecto de $*$ si, y sólo si, $(\forall y, z \in X)\,((x * y = x * z \rightarrow y = z) \wedge (y * x = z * x \rightarrow y = z))$ (si x tiene simétrico en X, entonces es simplificable en X).

Dadas dos l.c.i. $*$ y $\circ$ en X, decimos que $*$ satisface la `propiedad distributiva` respecto de $\circ$ en X si, y sólo si, $(\forall x, y, z \in X)\,(x * (y \circ z) = (x * y) \circ (x * z))$.

El concepto visto de l.c.i. u `operación diádica` (o, sinónimamente, `operación diargumental`), actuando sobre dos elementos, puede extenderse al caso general de n elementos. Una l.c.i. u `operación enádica` (o, sinónimamente, `operación n-ádica`, `operación enaria`, `operación n-aria`, `operación n-argumental` u `operación poliádica con n argumentos`) es una aplicación $f : X^n \longrightarrow X$, $\langle x_1, x_2, \ldots, x_n\rangle \longmapsto f(x_1, x_2, \ldots, x_n)$. Si se define con más de un argumento pero no especificamos su número decimos que es una `operación poliádica` (o, sinónimamente, `operación poliargumental`).

Decimos que un conjunto $X \neq \emptyset$ posee una estructura algebraica si, y sólo si, sobre él se define un número finito de leyes de composición, internas o externas. Suele decirse que X es el conjunto soporte de la estructura.

§ 4.1 Homomorfismos

Dadas dos estructuras algebraicas $(X; *)$ e $(Y; \circ)$, decimos que una aplicación $f : X \longrightarrow Y$ es un homomorfismo de $(X; *)$ en $(Y; \circ)$ si, y sólo si, $(\forall x, y \in X)\,(f(x * y) = f(x) \circ f(y))$. Un homomorfismo f se denomina: monomorfismo si, y sólo si, f es inyectiva; epimorfismo si, y sólo si, f es sobreyectiva; isomorfismo si, y sólo si, f es biyectiva; endomorfismo si, y sólo si, X e Y son el mismo conjunto y $*$ y $\circ$ son la misma operación; automorfismo si, y sólo si, f es endomorfismo e isomorfismo.

Siendo f un homomorfismo de $(X; *)$ en $(Y; \circ)$, llamamos imagen homomorfa de $(X; *)$ a la estructura algebraica $(f(X); \circ)$.

§ 4.2 Magma, semigrupo, monoide y grupo

Estas cuatro son estructuras con una sola l.c.i. Sean X un conjunto no vacío y $*$ una ley de composición en X. Decimos que: 0.º, $(X; *)$ es un magma si, y sólo si, $*$ una l.c.i. en X; 1.º, $(X; *)$ es un semigrupo si, y sólo si, $*$ es asociativa en X; 2.º, $(X; *)$ es un monoide si, y sólo si, $(X; *)$ es un semigrupo unitario (esto es, un semigrupo con elemento neutro), y 3.º, $(X; *)$ es un grupo si, y sólo si, $(X; *)$ es un monoide en el que todo elemento tiene simétrico. Con frecuencia se utiliza la letra G para los grupos, por ejemplo: «sea $(G; *)$ un grupo en el que...».

En general, una estructura $(X; *)$ tal que $*$ tiene elemento neutro en X, decimos que es una estructura unitaria. A veces se indica en la propia notación utilizando una tripleta $(X; *, 1)$. Una estructura $(X; *)$ tal que $*$ es conmutativa en X, decimos que es una estructura abeliana (o, sinónimamente, estructura conmutativa); así, por ejemplo, pudiésemos decir: «sea $(M; *, 1)$ un magma unitario abeliano tal que...».

§ 4.3 Anillo, anillo unitario, dominio de integridad y cuerpo

Estas cuatro son estructuras con dos leyes de composición internas.

Decimos que la estructura $(X; \oplus, \otimes)$ es un anillo si, y sólo si, X es un conjunto no vacío y $\oplus$ y $\otimes$ son dos l.c.i. (frecuentemente llamadas adición y multiplicación —o sinónima y respectivamente, suma y producto—) tal que se satisface: 0.º, $(X; \oplus)$ es un grupo abeliano; 1.º, $(X; \otimes)$ es un semigrupo, y 2.º, $\otimes$ es distributiva respecto de $\oplus$.

Decimos que un anillo $(X; \oplus, \otimes)$ es un anillo unitario si, y sólo si, $(X; \otimes)$ es un monoide.

Es costumbre relajar la notación utilizando los signos habituales de suma y producto, $+$ y $\cdot$, a la par que 0 designe el elemento neutro de $+$ (en vez de, digamos, $e_{\oplus}$ si siguiésemos utilizando $\oplus$) y 1 el de $\cdot$ (en vez de, digamos, $e_{\otimes}$ si siguiésemos utilizando $\otimes$) —a veces se indica en la propia notación utilizando una cuaterna $(X;+,\cdot,1)$—; por otro lado, es frecuente utilizar las letras A o R (del inglés *ring*) para el conjunto soporte de un anillo; así, por ejemplo, diríamos: «sea $(A;+,\cdot,1)$ un anillo unitario en el que…».

Un anillo $(A;+,\cdot)$ es un `anillo abeliano` o conmutativo si, y sólo si, $\cdot$ es conmutativa en A.

Llamamos `anillo íntegro` (o, sinónimamente, `dominio de integridad`) a todo anillo unitario abeliano sin divisores de cero, esto es, tal que $(\forall x,y\in A)(x\cdot y=0\rightarrow x=0\vee y=0)$.

Ejemplo 0

$(\mathbb{Z};+,\cdot)$, $(\mathbb{Q};+,\cdot)$, $(\mathbb{R};+,\cdot)$ y $(\mathbb{C};+,\cdot)$ son anillos íntegros.

Un `cuerpo` es un anillo unitario $(A;+,\cdot)$ con $1\neq 0$ en el que $(A\setminus\{0\};\cdot)$ es un grupo (todo elemento no nulo —distinto del neutro de $+$— tiene simétrico). Es frecuente utilizar las letras K (del alemán *körper*) o F (del inglés *field*) para el conjunto soporte de un cuerpo. Decimos que un cuerpo $(K;+,\cdot)$ es un `cuerpo abeliano` (o, sinónimamente, `cuerpo conmutativo`) si, y sólo si, $\cdot$ es conmutativa en K.

Ejemplo 1

$(\mathbb{Q};+,\cdot)$, $(\mathbb{R};+,\cdot)$ y $(\mathbb{C};+,\cdot)$ son cuerpos conmutativos.

§ 4.4 Retículo, retículo distributivo, retículo acotado, retículo complementado y álgebra de Boole

Un `retículo` es un conjunto X provisto de dos operaciones $\sqcup$ y $\sqcap$ asociativas y conmutativas y ambas satisfaciendo las leyes simplificativas: $(\forall x,y\in X)\ (x\sqcup(x\sqcap y)=x)$, de $\sqcup$ respecto de $\sqcap$, y $(\forall x,y\in X)\ (x\sqcap(x\sqcup y)=x)$, de $\sqcap$ respecto de $\sqcup$. Suele utilizarse la letra L (del inglés *lattice*) para el conjunto soporte de un retículo.

En todo retículo $(L;\sqcup,\sqcap)$ puede definirse el orden parcial $\leq$: $x\leq y\leftrightharpoons x\sqcup y=y$ (o equivalentemente, $x\leq y\leftrightharpoons x\sqcap y=x$). Es por esto por lo que una definición alternativa de retículo es la siguiente: un retículo es un conjunto parcialmente ordenado en el que cada dos elementos tienen un único supremo y un único infimo.

Ejemplo 2

Los números naturales ordenados parcialmente por divisibilidad, donde el supremo es el mínimo común múltiplo y el ínfimo el máximo común divisor, presentan estructura de retículo.

Un retículo $(L; \sqcup, \sqcap)$ es un retículo distributivo precisamente si se satisfacen (bastaría con que se satisficiese una de las dos) las leyes distributivas: $(\forall x, y, z \in L)\ (x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z))$, de $\sqcup$ respecto de $\sqcap$, y $(\forall x, y, z \in L)\ (x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z))$, de $\sqcap$ respecto de $\sqcup$.

Un retículo $(L; \sqcup, \sqcap)$ es un retículo acotado precisamente si existe el elemento neutro de $\sqcup$, 0 tal que $(\forall x \in L)\ (0 \sqcup x = x)$ (resultando que 0 es cota inferior para el orden anterior) y el elemento neutro de $\sqcap$, 1 tal que $(\forall x \in L)\ (1 \sqcap x = x)$ (resultando que 1 es cota superior para el orden anterior).

Un retículo acotado $(L; \sqcup, \sqcap)$ es un retículo complementado precisamente si se satisfacen las leyes de complementación, esto es, $(\forall x \in L)\ (\exists x' \in L)\ ((x \sqcup x' = 1) \wedge (x \sqcap x' = 0))$.

Llamamos álgebra de Boole a todo retículo distributivo y complementado. Es frecuente utilizar la letra B para el conjunto soporte de un álgebra de Boole.

§ 5 De la cardinalidad

Decimos que dos conjuntos son equinumerosos, notado $X \cong Y$, precisamente si existe una aplicación biyectiva entre X e Y. En este caso también decimos que X e Y tienen el mismo *(número) cardinal*, cardinalidad o *potencia*. Caso de ser X equinumeroso con algún subconjunto de Y pero no exista ningún subconjunto de X equinumeroso con Y decimos que el cardinal de X es *menor* que el cardinal de Y. La relación de equinumerosidad es de equivalencia y de orden parcial.

Decimos que X es un conjunto finito si, y sólo si, es vacío o, equivalentemente, si, y sólo si, es equinumeroso con el conjunto $\{0, 1, \ldots, n-1\}$, para algún $n \in \mathbb{N}$. Un conjunto infinito es un conjunto que no es finito. Se satisface que un conjunto es infinito si, y sólo si, es equinumeroso con alguna parte propia suya.

Decimos que un conjunto infinito X es un conjunto numerable si $\mathbb{N}$ y X son equinumerosos. $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ son numerables. Decimos que el (número) cardinal o potencia de un conjunto numerable es $\aleph_0$. El cardinal de $2^{\mathbb{N}}$ es $2^{\aleph_0}$. Se satisface que $\mathbb{R} \ncong \mathbb{N}$ y que $\mathbb{R} \cong 2^{\mathbb{N}}$. El cardinal de $\mathbb{R}$ (y de $2^{\mathbb{N}}$), notado $\mathfrak{c}$ (que no es otro que $2^{\aleph_0}$), lo llamamos el cardinal del continuo. De cualquier conjunto equinumeroso con $\mathbb{R}$ (y por tanto, con $2^{\mathbb{N}}$), decimos que su cardinal es $\mathfrak{c}$ (o sea, $2^{\aleph_0}$) y que tiene la potencia del continuo.

Decimos que un conjunto es *contable* si es finito o numerable[58]. Se satisface que cualquier subconjunto de un conjunto numerable es contable.

Una sucesión indizada de elementos de un conjunto X es una aplicación $s : I \longrightarrow X$ donde I es un conjunto preordenado; por lo general, notamos $s(i)$ por s_i y llamamos sucesión al rango de esta función, esto es, a $\{s_i, s_j, s_k, \ldots\}$. El conjunto de índices I puede ser infinito o finito. Una sucesión (numerable) de elementos de un conjunto X es una aplicación $s : \mathbb{N} \longrightarrow X$. Una sucesión

[58] Existen textos en los que los conjuntos que en estas notas llamamos numerables y contables, se denominan infinitos numerables y numerables, respectivamente.

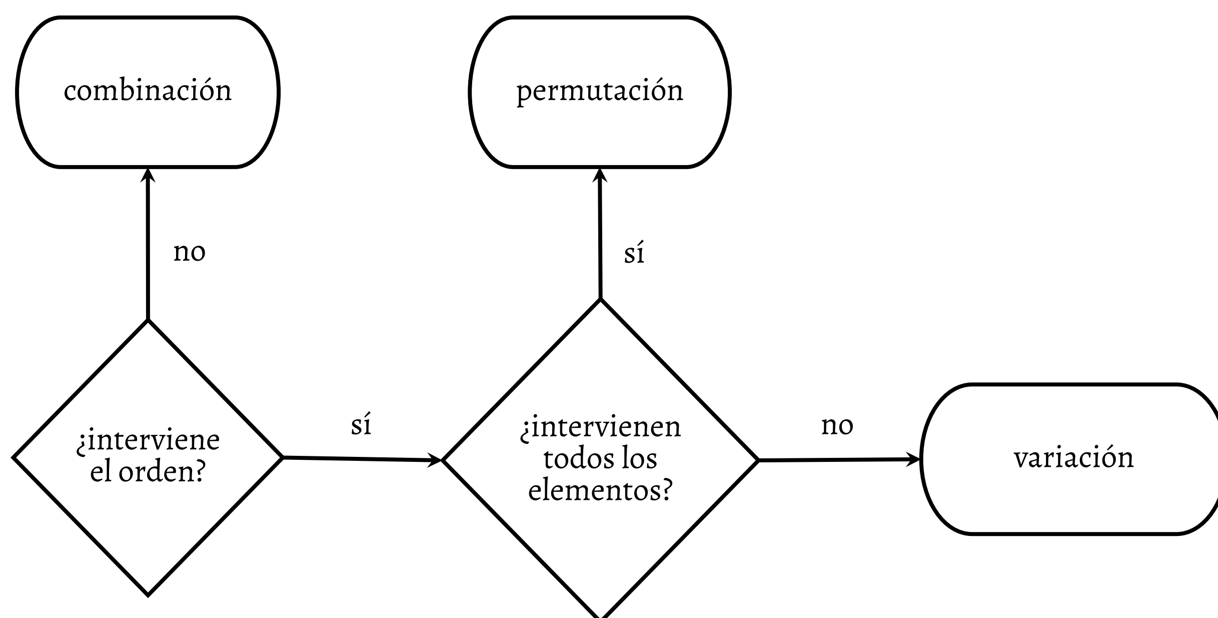
finita de elementos de X es una aplicación de $\emptyset$ o de $\{0, 1, \ldots, n-1\}$ en X que, en definitiva, equivale a una tupla enádica. Por esto último, también es habitual notar una sucesión por una tupla infinita $\langle s_0, s_1, \ldots \rangle$ —o simple y sinónimamente, por $\langle s_i \rangle_{i \geq 0}$— y una sucesión finita por una tupla finita, por ejemplo, $\langle s_0, s_1, \ldots, s_{n-1} \rangle$.

§ 6 De la combinatoria

Estudiadas en la educación secundaria, recordamos aquí las nociones de variación, permutación y combinación.

Una variación de k elementos de un conjunto no vacío X es cualquier aplicación inyectiva de $\{1, 2, \ldots, k\}$ en X. Una permutación de los elementos de un conjunto finito X es cualquier aplicación biyectiva de X en X. Una combinación de k elementos de un conjunto no vacío X es cualquier subconjunto de X de k elementos.

Aprendimos a distinguir ingenuamente entre ellas haciéndonos un par de preguntas.



Ejemplo 3

Dado el conjunto $C = \{a, b, c\}$, proporcionemos ejemplos de combinación, variación y permutación.

Resolución.— Dado el conjunto $C = \{a, b, c\}$, ejemplo de combinación de dos elementos de C es cualquier subconjunto de C (recordemos, $\{a, c\} = \{c, a\}$), ejemplo de variación de dos elementos de C es cualquier par ordenado de elementos de C (recordemos, $\langle a, c \rangle \neq \langle c, a \rangle$) y ejemplo de permutación de los elementos de C es cualquier terna (observemos que una permutación de los elementos de un conjunto de n elementos es una variación de n elementos de dicho conjunto). ■

§ 7 De los alfabetos y lenguajes

Suele definirse un alfabeto como un conjunto finito no vacío Σ, cuyos elementos son signos, frecuentemente llamados letras sujetas a la restricción de que Σ *no puede contener letras que sean hileras que comienzan con otras letras de* Σ. Así, permitiríamos $\Sigma = \{a, b, c\}$, $\Sigma = \{a, b, ca\}$, $\Sigma = \{a, b, Ab\}$, pero no, por ejemplo, $\Sigma = \{a, b, c, ca\}$.

Dado un alfabeto Σ, una palabra (o, sinónimamente, cadena) es cualquier hilera finita de letras de Σ, esto es, cualquier sucesión finita de letras de Σ indizada por un conjunto finito ordenado, por ejemplo, $\{0, 1, \ldots, n-1\}$. Si $\Sigma = \{a, b, c\}$, una palabra es $\langle a, b, b, c, c, c, a, a\rangle$ (indizada por $\{0, 1, \ldots, 7\}$, esto es, por ejemplo, la letra 0.ª es a, la letra 1.ª es b, …, la letra 7.ª es a). Es habitual no explicitar el formato de tupla en las palabras; por ejemplo, la anterior se abrevia $abbcccaa$. Por ε_Σ o simplemente ε, designamos la palabra vacía (o, sinónimamente, nula) (que si es necesario podría interpretarse como una sucesión finita indizada por $\emptyset$).

Un segundo conjunto destacado es el conjunto de todas las palabras que usan exclusivamente letras de Σ; este nuevo conjunto lo designamos Σ^* y se conoce como la clausura de Kleene[59]. Por ejemplo, si $\Sigma = \{a, b\}$, $\Sigma^* = \{\varepsilon, a, b, ab, ba, aba, abb, baa, bab, abaa, \ldots\}$.

Es habitual representar las palabras por las letras s, t, u, v, w, x, y, z, o también por letras del alfabeto griego.

Definimos la longitud de una palabra ω de Σ^* y notamos $\operatorname{long}(\omega)$ (o, sinónimamente, $|\omega|$), como el número de letras de Σ en ω, contando cada letra que aparezca; $|\varepsilon| = 0$. La longitud de una letra de Σ es 1. La longitud de $abbcccaa$ es 8.

Igual que dos letras se yuxtaponen y forman una palabra, pueden yuxtaponerse dos palabras para dar lugar a una nueva. En general, llamamos *concatenar palabras* a esto.

Dadas dos palabras $u, v \in \Sigma^*$, definimos la concatenación de u, de longitud h y v, de longitud k, como la palabra w, de longitud $h + k$, definida por

$$w(i) = \begin{cases} u(i) & \text{si } 0 \leq i \leq h-1, \\ v(i-h) & \text{si } h \leq i \leq h+k-1. \end{cases}$$

No existe una notación estándar para la concatenación de palabras; es habitual expresar la concatenación de u y v sin ningún signo uv (aunque también con alguno, por ejemplo, $u + v$, $u \mathbin{+\!\!+} v$, $u^\frown v$ o $u||v$, entre otras formas).

Designamos por ω^k la concatenación de la palabra ω consigo misma k veces; $\omega^0 = \varepsilon$ y $\omega^k = \omega\omega^{k-1}$.

[59] *Vid. v. gr.* https://es.wikipedia.org/wiki/Clausura_de_Kleene.

Definida la concatenación, ésta es la `definición inductiva de` Σ^*:

0. la palabra vacía está en Σ^*;

1. si ω está en Σ^* y x está en Σ, entonces ωx está en Σ^*.

Definición que reescribimos:

0. $\Sigma_0 = \{\varepsilon\}$;

1. $\Sigma_i = \{\omega x : \omega \in \Sigma_{i-1} \wedge x \in \Sigma\}$ (para $1 \leq i$);

2. $\Sigma^* = \bigcup_{i \in \mathbb{N}} \Sigma_i$.

Diremos que la concatenación genera `compuestos de palabras`.

Una palabra v es un `elemento de un compuesto` u (o, sinónimamente, una `subpalabra` de u) precisamente si existen dos palabras s y t tales que $u = svt$, en cuyo caso, si $u \neq v$ (esto es, si ni s ni t son la palabra vacía), decimos que v es un `elemento compositivo propio` del compuesto u. Los elementos s y t se conocen como `(sub)(palabra) prefijo` y `(sub)(palabra) sufijo` de u, respectivamente. Designamos por $v_{[k]}$ el prefijo de v de longitud k y por $v^{[k]}$ el sufijo de v de longitud k.[60]

Ejemplo 4

Desglosemos el compuesto «correveidile» en español.

Resolución.— Siendo Σ el alfabeto del idioma español, en la palabra u = «correveidile» pueden considerarse, por ejemplo, el elemento compositivo propio v = «ve», el prefijo p = «corre» y el sufijo p = «idile» compuesto a su vez, por ejemplo, por el prefijo «i», el sufijo «le» y el elemento compositivo propio «di». ■

Se demuestra que $(\Sigma^*; +\!\!+)$ es un *monoide* (ε es el elemento neutro, es decir, satisface que para toda u de Σ^*, $\varepsilon u = u\varepsilon = u$). Dicho monoide no es abeliano si $|\Sigma| \geq 2$.

También tenemos la `definición recursiva de la longitud`:

0. $|\varepsilon| = 0$;

1. dada ω en Σ^*, si $|\omega|$ ha sido definida y x está en Σ, entonces $|\omega x| = |\omega| + 1$.

Un tercer conjunto destacado es el de todas las palabras de longitud k, que notamos Σ^k.

[60] En ingeniería de la computación es habitual hablar de cadenas en vez de palabras, por lo que este párrafo podría leerse como reza a continuación. Una cadena v es una `subcadena` de una cadena u precisamente si existen dos cadenas s y t tales que $u = svt$, en cuyo caso, si $u \neq v$ (esto es, si ni s ni t son la cadena vacía), decimos que v es una `subcadena propia` de la cadena u. Las subcadenas s y t se conocen como la `subcadena prefijo` y la `subcadena sufijo` de u, respectivamente.

Un lenguaje de alfabeto Σ es cualquier subconjunto de Σ^*. A Σ^* se le conoce como el lenguaje universal de alfabeto Σ. Por ejemplo, si $\Sigma = \{0, 1\}$, el lenguaje universal es $\Sigma^* = \{\varepsilon, 0, 1, 01, 10, 010, 011, 100, 101, 0100, \ldots\}$ y ejemplos de lenguajes son $\{10, 11, 101, 111, 1011, 1100101\}$ (un lenguaje finito) y $\{10, 11, 101, 111, 1011, 1101, 10001, 10011, \ldots\}$ (un lenguaje infinito), ambos subconjuntos propios de Σ^*.

§ 8 De los grafos

§ 8.0 Vértices y enlaces de un grafo

Un grafo $G = (V, E)$ consiste en un conjunto V de vértices (o, sinónimamente, nodos) y un conjunto E de enlaces (o, sinónimamente, ejes). Los enlaces se representan gráficamente con líneas (cuya forma nos será indiferente; sólo importará qué vértices unen y si están orientadas o no).

Dos o más enlaces con los mismos extremos se llaman enlaces múltiples (o, sinónimamente, enlaces paralelos). Si un grafo admite enlaces múltiples, decimos que es un multigrafo; si admite n enlaces entre cada dos vértices, decimos que es un n-grafo.

Un enlace bucle (o, sinónimamente, enlace lazo o, simplemente, bucle o lazo) es aquél que tiene un solo extremo (conecta un vértice consigo mismo)[61].

Un grafo simple es aquél que no tiene enlaces múltiples ni bucles. Un grafo ponderado (resp., multigrafo ponderado) es un grafo (resp., multigrafo) con una función $w : E \longrightarrow \mathbb{R}$ que asigna un peso a cada enlace.

§ 8.1 Subgrafo de un grafo

Decimos que un grafo $H = (W, F)$ es un subgrafo de un grafo G precisamente si todos los vértices y todas las aristas de H lo son también de G —esto es, si $W \subseteq V$ y $F \subseteq E$— y si todos los nodos extremos de los enlaces de F están en W. Se trata de un subgrafo propio precisamente si $F \neq E$. Si $W = V$ se dice que es un subgrafo de expansión. El subgrafo inducido en un conjunto $W \subseteq V$ es el subgrafo constituido por todos los enlaces cuyos extremos están en W; suele designarse por $\langle W \rangle$.

§ 8.2 Caminos en un grafo

Un camino (*walk*) es una secuencia alternante de vértices y enlaces $v_0 e_0 v_1 e_1 \ldots v_n e_n v_{n+1}$, con $n \geq 0$; se trata de un camino cerrado precisamente si $v_0 = v_{n+1}$ (por ejemplo, $v_0 e_0 v_0$ con e_0 un enlace bucle) y de un camino abierto en caso contrario; decimos de v_0 y v_{n+1} que son vértices

[61] En algunos textos, si un grafo presenta bucles, dicen de él que es un seudografo.

conectados; la longitud de un camino es el número de enlaces que contiene[62]; si la conexión entre v_0 y v_{n+1} es por un camino de longitud 1, se denominan vértices adyacentes (en otras palabras, son dos vértices conectados por un enlace); un enlace incidente a un vértice es un enlace que lo conecta; en tal caso, el vértice es un extremo del enlace (como ya hemos hecho, representamos el enlace e que incide —o, sinónimamente, conecta— los vértices u y v por uev); un vértice colgante está conectado exactamente a otro vértice mediante un solo enlace; de un vértice que no está conectado con ningún otro vértice distinto de él, decimos que es un vértice aislado.

Un sendero (*trail*) es un camino sin enlaces repetidos; un camino simple (*path*) es un sendero sin vértices repetidos (y, por lo tanto, sin enlaces repetidos); un sendero es un sendero euleriano precisamente si recorre todos los enlaces del grafo exactamente una vez.

El camino de menor longitud entre dos nodos se denomina geodésica. La longitud de la geodésica de mayor longitud en un grafo se llama diámetro del grafo.

Un circuito es un sendero cerrado; un circuito trivial tiene un solo vértice y ningún enlace; un grafo es un grafo euleriano precisamente si contiene un circuito euleriano; un ciclo es un circuito no trivial en el que el único vértice repetido es el primero-último[63].

§ 8.3 Grafos isomorfos

Decimos que dos grafos simples G y H son grafos isomorfos precisamente si existe una biyección f entre sus vértices tal que $\{v, w\}$ es una arista en G si, y sólo si, $\{f(v), f(w)\}$ lo es en H.

Teorema -1.0

Dos grafos isomorfos deben tener:

0. El mismo número de vértices.
1. El mismo número de enlaces.
2. El mismo número de vértices para cada grado dado.
3. El mismo número de ciclos.
4. El mismo número de ciclos de cualquier tamaño dado.

§ 8.4 Grafos conexo, completo y r-regular

Un grafo conexo es aquél en el que todas las parejas de vértices lo son de vértices conectados, en otras palabras, aquél en el que existe un camino entre cada dos nodos. Una componente conexa de un grafo G es un subgrafo conexo máximo suyo, esto es, no contenido en ningún otro subgrafo conexo de G.

[62] Se dice de un camino de longitud cero que es un camino trivial.

[63] Observemos que un circuito no permite enlaces repetidos, aunque sí vértices repetidos, mientras que un ciclo no permite vértices repetidos (excepto el primero-último), aunque sí enlaces repetidos; pudiésemos decir que un ciclo es un camino simple cerrado.

Teorema -1.1
Sea G un grafo conexo; entonces G es euleriano si, y sólo si, todos sus vértices tienen grado par.

Teorema -1.2
Un grafo conexo no euleriano tiene un sendero euleriano si, y sólo si, tiene exactamente dos vértices de grado impar. El sendero comienza y termina en dichos vértices.

Un `grafo completo` es aquél en el que cada vértice es adyacente a todos los otros vértices. El grafo completo de n vértices lo notamos K_n. El grafo K_n tiene $n(n-1)/2$ enlaces.

El `grado` de un vértice v es el número de enlaces incidentes en él; lo notamos $\mathrm{gr}(v)$. Un grafo `r-regular` es un grafo simple cuyos vértices, todos, tienen grado r. El grafo K_n es $(n-1)$-regular.

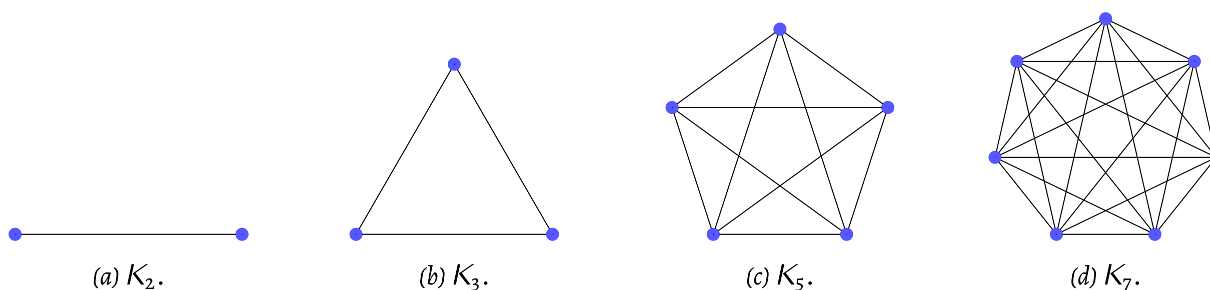
Teorema -1.3 (Lema del apretón de manos)
En todo grafo con n vértices v_i y m enlaces, se cumple:

$$\sum_{i=1}^{n} \mathrm{gr}(v_i) = 2m.$$

Ejemplo 5

Dibujemos, salvo isomorfismos, los grafos completos K_2, K_3, K_5 y K_7.

Resolución.— Dibujémoslos:



(a) K_2. (b) K_3. (c) K_5. (d) K_7.

Figura 0.— Grafos completos K_2, K_3, K_5 y K_7.

Éstos son. ■

§ 8.5 Grafo dirigido

Si en un conjunto A actúa una relación diádica R, según sea ésta, distinguimos entre `grafo no dirigido` (o, sinónimamente, `grafo no orientado`) si R es simétrica en A, y `grafo dirigido` (o,

sinónimamente, `grafo orientado` o `digrafo`) si R no es simétrica en A. El grafo queda identificado por el conjunto y la relación, esto es, $G = (A; R)$.

En los grafos no dirigidos, los enlaces se denominan `aristas` (enlaces no orientados); en los grafos dirigidos, `arcos` (enlaces orientados —se recorren en un solo sentido—); representamos alternativamente los arcos con pares ordenados $\langle u, v\rangle$ y decimos que u es un `vértice adyacente a` v y que v es un `vértice adyacente desde` u (si se trata de aristas en vez de arcos, se habla simplemente de *vértices adyacentes*). En la gráfica del grafo, el arco $\langle u, v\rangle$ se representa con una flecha de u a v, mientras que una arista con una línea.

Optativamente, pudiésemos utilizar en grafos dirigidos tal adjetivo, por ejemplo, `camino (dirigido)`, `sendero (dirigido)`, y así. Sin embargo, hemos de saber que el concepto de `camino dirigido` existe en un grafo cualquiera, como aquél camino cuyos enlaces están todos orientados en un mismo sentido.

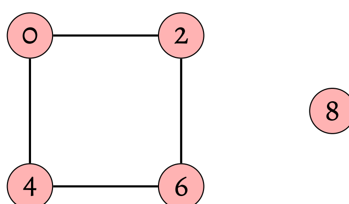
En un grafo dirigido, el `grado de entrada` de un vértice es el número de arcos que llegan al mismo, y el `grado de salida` de un vértice es el número de arcos que parten de él.

Un grafo dirigido es `fuertemente conexo` precisamente si entre cualesquiera dos vértices u y v, existe un camino simple dirigido de u a v y un camino simple dirigido de v a u.

Ejemplo 6

Dibujemos, salvo isomorfismos, el grafo no dirigido $G = (A, R)$, con $A = \{0, 2, 4, 6, 8\}$ y $R = \{\langle 0, 2\rangle, \langle 0, 4\rangle, \langle 2, 0\rangle, \langle 2, 6\rangle, \langle 4, 0\rangle, \langle 4, 6\rangle, \langle 6, 2\rangle, \langle 6, 4\rangle\}$.

Resolución.— Dibujémoslo:

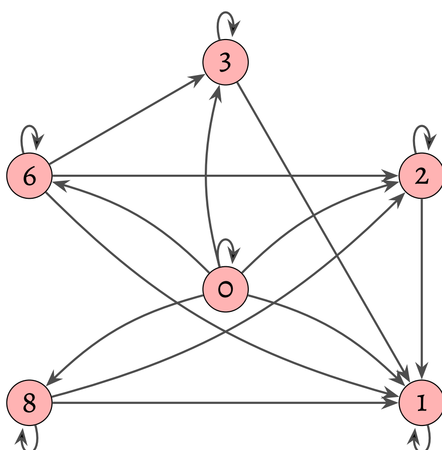


Éste es. ■

Ejemplo 7

Dibujemos, salvo isomorfismos, el grafo dirigido $G = (A; R)$, con $A = \{0, 1, 2, 3, 6, 8\}$ y R, definida en A por $xRy \leftrightarrow x$ es múltiplo de y.

Resolución.— Dibujémoslo:



Éste es. ■

§ 8.6 Reducciones reflexiva y transitiva de un grafo

Llamamos `reducción reflexiva de un grafo` G a un nuevo grafo que resulta de suprimir los bucles en el grafo G. Llamamos `clausura transitiva de un grafo` G a un nuevo grafo que contiene el enlace $\langle u, v\rangle$ siempre que existe un camino dirigido de u a v en G. Llamamos `reducción transitiva de un grafo` G al menor grafo con la misma clausura transitiva que G.

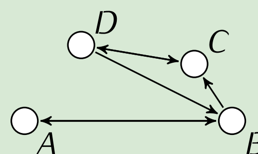
§ 8.7 Matriz de adyacencia de un grafo

La `matriz de adyacencia` (o, sinónimamente, `matriz de conexiones`) de un grafo es una matriz cuadrada de ceros y unos en la que un uno representa que los vértices correspondientes a los índices son adyacentes, y un cero que no lo son.

Ejemplo 8

El grafo adjunto representa las conexiones entre cuatro estaciones de tranvía. Hagamos lo siguiente:

0. escribamos la matriz de adyacencia G de dicho grafo;
1. interpretemos las matrices G^2 y G^3;
2. razonemos si dicho grafo es o no fuertemente conexo.



[Cubit 164].

Resolución.— 0. La matriz de adyacencia G de dicho grafo es:

$$G = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Formalizamos la matriz de adyacencia del grafo, haciendo corresponder los subíndices posicionales 0, 1, 2 y 3 de sus elementos a las etiquetas A, B, C y D. De esta forma, cada elemento g_{ij} de G indica si existe o no una conexión directa —sin paradas intermedias (caminos de longitud uno en el grafo)— entre las estaciones de tranvía correspondientes a i y j, en el sentido de i a j. Así, la igualdad $g_{12} = 1$ se interpreta como la existencia de una conexión directa de 1 a 2, esto es, de B a C, mientras que la igualdad $g_{21} = 0$ corresponde a la no existencia de una conexión directa de 2 a 1, esto es, de C a B.

1. Las potencias 2 y 3 de G son:

$$G^2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \quad \text{y} \quad G^3 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 2 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 2 & 1 & 1 \end{pmatrix}$$

Cada elemento $g_{ij}^{(2}$ de G^2 indica el número de conexiones con una estación intermedia (caminos de longitud dos en el grafo) desde la estación correspondiente a i a la estación correspondiente a j, según la formalización anterior. Similarmente, cada elemento $g_{ij}^{(3}$ de G^3 indica el número de conexiones con dos estaciones intermedias (caminos de longitud tres en el grafo) desde la estación correspondiente a i a la estación correspondiente a j, también según la formalización anterior.

2. Un grafo es fuertemente conexo precisamente si para cualquier par de nodos existe un camino que los une. El grafo en cuestión lo es, porque, si bien las matrices G y $G + G^2$ tienen elementos nulos —por ejemplo, g_{00} y $g_{03} + g_{03}^{(2}$—, la matriz $G + G^2 + G^3$ no los tiene:

$$G + G^2 + G^3 = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 2 & 3 & 1 \\ 1 & 1 & 2 & 2 \\ 1 & 3 & 3 & 2 \end{pmatrix}$$

lo que significa que dos estaciones cualesquiera están conectadas, sea directamente o indirectamente con una o dos paradas intermedias; en otras palabras, esta matriz nos informa de cómo ir de un vértice a otro sin que sucedan más de dos paradas.

De hecho, tampoco tiene elementos nulos la matriz $G^2 + G^3$:

$$G^2 + G^3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 2 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 2 & 2 & 2 \end{pmatrix}$$

esto es, cualesquiera dos estaciones están conectadas por trayectorias con una o dos paradas intermedias. ■

§ 8.8 Grafo bipartito

Decimos de un grafo que es un `grafo bipartito` si su conjunto de vértices puede particionarse en dos subconjuntos disjuntos S_0 y S_1, tal que toda enlace conecta un vértice de S_0 con uno de S_1.

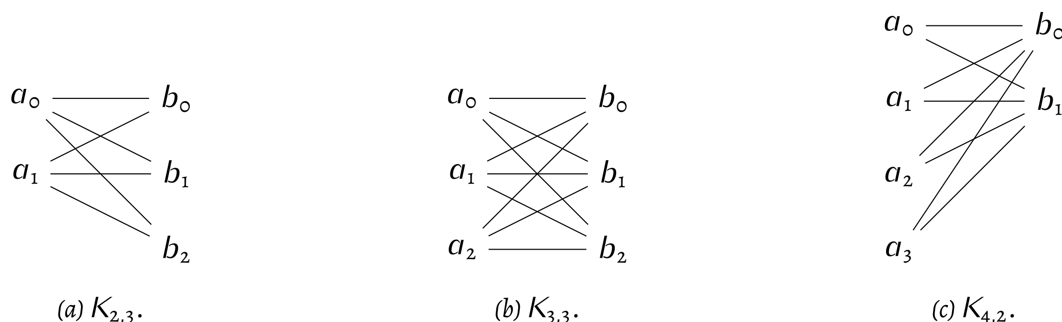
Si en un conjunto A actúa una relación diádica R, según sea ésta, distinguimos entre `grafo bipartito no dirigido` (o, sinónimamente, `grafo bipartito no orientado`) si R es simétrica en A, y `grafo bipartito dirigido` (o, sinónimamente, `grafo bipartito orientado` o `digrafo bipartito`) si R no es simétrica en A.

El `grafo bipartito completo` $K_{n,m}$ conecta cada vértice de $S_0 = \{a_0, \ldots, a_{n-1}\}$ con todos los de $S_1 = \{b_0, \ldots, b_{m-1}\}$.

Ejemplo 9

Dibujemos, salvo isomorfismos, los grafos bipartitos completos $K_{2,3}$, $K_{3,3}$ y $K_{4,2}$.

Resolución.— Dibujémoslos:



(a) $K_{2,3}$. (b) $K_{3,3}$. (c) $K_{4,2}$.

Figura 1.— Grafos bipartitos completos $K_{2,3}$, $K_{3,3}$ y $K_{4,2}$.

Éstos son. ■

§ 8.9 Grafo plano

Decimos que un grafo simple y conexo es un `grafo plano` si puede dibujarse en el plano sin que se crucen las líneas que representan sus enlaces. Tal representación se llama *incrustación del grafo en el plano*. Para una incrustación de un grafo en el plano, una `cara` del grafo es una región del plano creada por el dibujo. El área del plano fuera del grafo también es una cara, la `cara no acotada`.

Teorema -1.4 (Teorema de Kuratowski)
Un grafo G es no plano si, y sólo si, contiene una subestructura isomorfa a $K_{3,3}$ o a K_5 (una «copia» de uno de ellos).

Teorema -1.5 (Fórmula de Euler para grafos planos)
Para todo grafo conexo incrustado en el plano, con V vértices, E enlaces y F caras, se satisface:

$$V + F = E + 2.$$

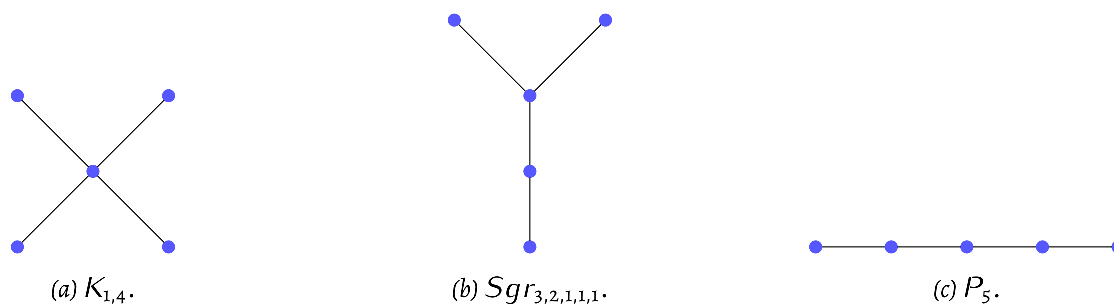
§ 9 De los árboles

Un `árbol` es un grafo simple, conexo y sin ciclos. De los vértices de grado 1 decimos que son las `hojas` del árbol.

Ejemplo 10

Dibujemos todos los árboles no isomorfos de cinco vértices.

Resolución.— Dibujémoslos:



(a) $K_{1,4}$. (b) $Sgr_{3,2,1,1,1}$. (c) P_5.

Figura 2.—Árboles $K_{1,4}$, $Sgr_{3,2,1,1,1}$ y P_5.

Estos tres son los únicos árboles no isomorfos de cinco vértices. ■

Un `árbol generador` de un grafo simple y conexo G es un subgrafo T que es un *árbol* y contiene todos los vértices de G.

Teorema -1.6
Si T es un *árbol* con n aristas, entonces tiene $n+1$ vértices.

Un `árbol generador mínimo` de un grafo ponderado es aquél con peso total mínimo entre todos los árboles generadores.

§ 9.0 De los árboles enraizados

Trabajaremos con un tipo particular de árboles, los árboles enraizados.

Definiciones

Por `árbol enraizado no ordenado` entendemos una colección formada por:

0. un conjunto S de elementos denominados `nodos` (o, sinónimamente, `vértices` o `puntos`);
1. una función l que asigna a cada nodo un número natural positivo $l(x)$ que llamamos `nivel` de x;
2. una relación $\prec$ definida en S —$\forall x, y \in S$, leemos $x \prec y$ como «x es un `ascendiente` (o, sinónimamente, `ancestro` o `predecesor`) de y» o «y es un `descendiente` (o, sinónimamente, `sucesor`) de x»[64]— que satisface:

   0.°, existe un único nodo de nivel 0, que llamamos `raíz` (o, sinónimamente, `origen` del árbol;

   1.°, todo nodo distinto de la raíz tiene un único predecesor, y

   2.°, para cualesquiera nodos x e y, si y es descendiente de x, entonces $l(x) = l(x) + 1$.

   Designamos por $\delta(x)$ el conjunto de descendientes de un nodo x.

   Decimos de un nodo x que:

- es un `nodo hoja` (o, sinónimamente, `nodo objetivo`) (o `nodo final` o `nodo terminal` del árbol) precisamente si no tiene descendientes, esto es, si, y sólo si, $\delta(x) = \emptyset$;
- es un `nodo interno` (o, sinónimamente, `nodo propio`) precisamente si tiene al menos un descendiente, esto es, si, y sólo si, $\delta(x) \neq \emptyset$;
- es un `nodo simple` precisamente si sólo tiene un descendiente, esto es, si, y sólo si, $\delta(x)$ es un subconjunto unitario de S;
- es un `nodo complejo` (o, sinónimamente, `nodo unión`) si tiene más de un descendiente, esto es, si, y sólo si, $\delta(x) \neq \emptyset$ y no unitario.

[64] Si la representación incluye herencia de características entre nodos podría distinguirse incluso entre descendiente y sucesor, considerando un sucesor un caso particular de descendiente que hereda determinadas características de nodos ancestros suyos.

Un camino es cualquier sucesión finita o infinita numerable de nodos tal que cualquier término de la sucesión es predecesor del siguiente, esto es cualquier conjunto totalmente ordenado de nodos $(\{x_i\}_{i\in I\subseteq\mathbb{N}}; \prec)$ (alternativamente, designaremos un camino por una tupla; por ejemplo, el camino $y \prec z \prec x$ lo designamos por la tupla $\langle y, z, x\rangle$). Si el camino es finito, hablamos de nodo inicial y nodo terminal (o, sinónimamente, nodo final) del camino y de su longitud, siendo ésta el número de nodos menos uno. Si el camino es infinito sólo hablamos de su nodo inicial y de su longitud (infinita numerable).

Un camino enraizado es cualquier camino que comience en el nodo raíz. De la definición de $\prec$ se sigue que para todo nodo x existe un único camino enraizado C_x cuyo último término es x. Si $y \in C_x$ decimos que y domina a x (o, sinónimamente, que x está dominado por y). Si y domina a x e $y \neq x$ decimos que y está por encima de x (o, sinónimamente, que y es de nivel superior a x) —o que x está por debajo de y (o, sinónimamente, que x es de nivel inferior a y)—. Decimos que x e y son comparables si x domina a y o viceversa. Decimos que un nodo z está entre dos nodos x e y si z está por encima de uno de ellos y por debajo del otro. Decimos que x es el ancestro directo/inmediato de y o que y es el descendiente directo/inmediato de x si no existe ningún nodo entre x e y.

Para un nodo, llamamos grado de entrada (o, sinónimamente, invalencia a su número de ancestros directos y grado de salida (o, sinónimamente, exvalencia o grado de ramificación) a su número de descendientes directos. El nodo raíz es el único nodo con grado de entrada cero y los nodos hoja son los únicos nodos con grado de salida cero. Llamamos grado (o, sinónimamente, valencia) de un nodo la suma de sus grados de entrada y de ramificación.

Un árbol enraizado finito es un árbol enraizado que tiene un número finito de nodos. Un árbol con un solo nodo lo llamamos árbol hoja (o, sinónimamente, árbol degenerado).

Una rama (o, sinónimamente, camino maximal) es un camino enraizado infinito o un camino enraizado que termina en un nodo hoja. En un árbol enraizado finito, todas las ramas son finitas y el número total de ellas es el número de hojas.

Llamamos profundidad (o, sinónimamente, nivel) de un nodo, a la longitud del camino enraizado del que es nodo terminal. Por ejemplo, si y es el descendiente directo de x, la profundidad de y es igual a la profundidad de x más uno. Llamamos altura de un árbol enraizado a la mayor profundidad, que será finita si el árbol enraizado es finito. Así, la altura de un árbol hoja es cero y la de un árbol infinito, infinita.

Un árbol enraizado finitamente generado es aquél en el que cada nodo tiene sólo un número finito de descendientes. Un árbol enraizado finitamente generado puede ser infinito.

Llamamos árbol enraizado de ramificación finita a todo árbol enraizado tal que el grado de ramificación de cualquiera de sus nodos es un número natural.

La siguiente es una condición suficiente par la existencia de ramas infinitas.

Teorema -1.7 (Lema de König)
Todo árbol infinito de ramificación finita contiene al menos una rama infinita.

Un árbol enraizado enario (o, sinónimamente, árbol enraizado n-ario o n-árbol enraizado) ($2 \leq n$) es un árbol enraizado en el que todo nodo propio tiene como máximo n descendientes directos. Si todo nodo propio tiene exactamente n descendientes directos decimos que es un árbol enraizado enario completo (o, sinónimamente, n-árbol enraizado completo). Cuando un un árbol enraizado enario completo es tal que todos sus nodos hoja son del mismo nivel decimos que es un árbol enraizado enario totalmente completo (o, sinónimamente, árbol regular. Si h es la altura de un árbol enraizado enario y todos sus nodos hoja son de nivel h o $h-1$ decimos que es un árbol enario equilibrado.

Actividad -1.0

Sea $T(S, l, \prec)$ un árbol enraizado enario completo, entonces:

0.°, si tiene p nodos propios, entonces tiene
- $np+1$ nodos y
- $(n-1)p+1$ hojas;

1.°, si tiene v nodos, entonces tiene
- $(v-1)/n$ nodos propios y
- $((n-1)v+1)/n$ hojas, y

2.°, si tiene j hojas, entonces tiene
- $(nj-1)/(n-1)$ nodos y
- $(j-1)/(n-1)$ nodos propios.

Un árbol enraizado ordenado es un árbol enraizado no ordenado junto a una función δ que asigna a cada nodo unión x la tupla o sucesión $\delta(x)$ de nodos descendientes de x; en otras palabras, un árbol enraizado no ordenado tal que $(\delta(x); \prec)$ es un conjunto totalmente ordenado.

Del árbol enraizado ordenado que es tal que cada uno de sus nodos unión sólo tiene dos descendientes directos decimos que es un árbol enraizado (ordenado) diádico (o, sinónimamente, a veces, árbol enraizado binario). Dado un nodo unión en un árbol enraizado diádico, el primer descendiente directo lo denominamos descendiente izquierdo y el segundo, descendiente derecho.

Tenemos dos árboles enraizados isomorfos, $T_0 = (S_0, l_0, \prec_0)$, de raíz r_0 y $T_1 = (S_1, l_1, \prec_1)$, de raíz r_1, precisamente cuando existe una biyección $f : S_0 \longrightarrow S_1$ tal que:

0.°, $f(r_0)$ es el nodo raíz de T_1 (transforma el nodo raíz de T_0 en el nodo raíz de T_1), y

1.°, $\forall x \in S_0$, tal que $\delta(x) = \{x_i\}_{i \in I}$, entonces $f(\delta(x)) = \{f(x_i)\}_{i \in I}$ (transforma el conjunto de descendientes de $x \in S_0$ en el conjunto de descendientes de $f(x) \in S_1$).

En el caso de árboles enraizados ordenados isomorfos, f es un isomorfismo de orden[65] entre los conjuntos totalmente ordenados $(\delta(x); \prec_0)$ y $(f(\delta(x)); \prec_1)$, esto es, si, y sólo si, $\forall i, j \in I$, $x_i \prec_0 x_j \Leftrightarrow f(x_i) \prec_1 f(x_j)$.

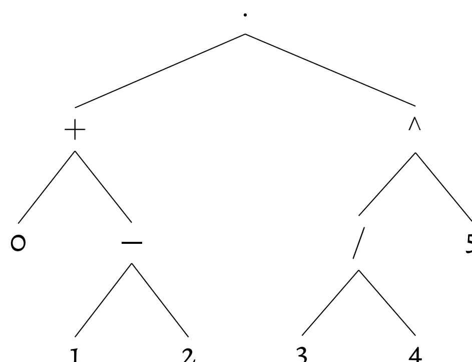
Árboles sintácticos

Un árbol sintáctico[66] es un árbol enraizado diádico que se compone de varios nodos integrados en una estructura jerárquica y representa una expresión bien formada de un campo sintáctico determinado.

Ejemplo 11

Dibujemos el árbol sintáctico que representa la expresión aritmética $(0 + (1 - 2)) \cdot (3/4)^5$ y expliquemos por qué la representa.

Resolución.— La representación de la expresión aritmética $(0 + (1 - 2)) \cdot (3/4)^5$ mediante un árbol sintáctico, construido ascendentemente, con las operaciones situadas en los nodos raíz de los diferentes subárboles y los operandos en los nodos hoja:



El primer nodo del árbol sintáctico etiquetado «·» es un producto e indica el *tipo* de la expresión, en este caso, aritmética. Esta expresión tiene dos ramas correspondientes a las dos subexpresiones argumentos del producto. Las etiquetas «+» e «∧» de los nodos de cada rama nos dicen el tipo de dichas subexpresiones, en este caso, la primera, aritmética y la segunda, lógica. Y así sucesivamente hasta llegar a las hojas del árbol, que en este ejemplo son números enteros. ■

Es posible recuperar la expresión representada a partir del árbol sintáctico invirtiendo el proceso de construcción. Tal y como lo hemos construido, la forma de proceder se le conoce como recorrido en orden del árbol[67]. Recorrer en orden es recorrer de izquierda a derecha y de abajo arriba.

[65] *Cfr. infra* ejemplo 6 (pág. 700 de esta edición).

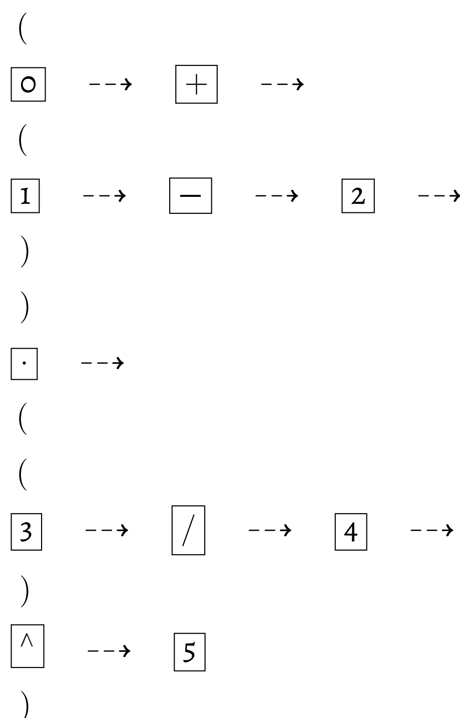
[66] En inglés también se conoce por *expression tree*.

[67] Hay más formas de recorrer un árbol diádico (*vid. v. gr.* https://es.wikipedia.org/wiki/Árbol_binario#Recorridos_sobre_árboles_binarios).

Ejemplo 12

Recorramos en orden el árbol del ejemplo anterior.

Resolución.— El recorrido en orden del árbol diádico anterior es



Del recorrido en orden del árbol obtenemos una expresión en `forma infija`; en este ejemplo:

$$(0 + (1 - 2)) \cdot ((3/4)^{\wedge}5).$$ ■

Observación 9.0.— Pudiésemos utilizar el artefacto en línea SageMath[68] y el siguiente programita en lenguaje Sage para hallar la expresión en forma infija a partir de recorrer en orden su árbol sintáctico,

[68] *Cfr. supra* § 11 (pág. cii de esta edición).

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/

class Nodo:
        def __init__(self, valor, izquierdo=None, derecho=None):
                self.valor = valor
                self.izquierdo = izquierdo
                self.derecho = derecho

def recorrido_enorden(nodo):
        if nodo is not None:
                if nodo.izquierdo or nodo.derecho:
                        print("(", end=" ")  # abre paréntesis si no es hoja
                recorrido_enorden(nodo.izquierdo)
                print(nodo.valor, end=" ")  # imprime el nodo actual
                recorrido_enorden(nodo.derecho)
                if nodo.izquierdo or nodo.derecho:
                        print(")", end=" ")  # cierra paréntesis si no es hoja

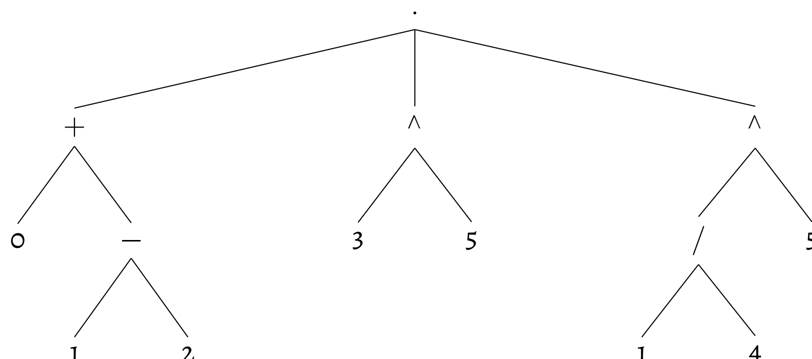

    # construyendo el árbol sintáctico
    raiz = Nodo("*",
            Nodo("+",
                    Nodo(0),
                    Nodo("-",
                            Nodo(1),
                            Nodo(2)
                    )
            ),
            Nodo("^",
                    Nodo("/",
                            Nodo(3),
                            Nodo(4)
                    ),
                    Nodo(5)
            )
    )

    # mostrando la expresión en forma infija
    print("Expresión en forma infija (resultado del recorrido en orden):")
    recorrido_enorden(raiz)
    print()
```

Su ejecución proporciona:

```
Expresión en forma infija (resultado del recorrido en orden):
( ( 0 + ( 1 - 2 ) ) * ( ( 3 / 4 ) ^ 5 ) )
```

Observación 9.1.— También pudiésemos utilizar un árbol triádico, construido similarmente. Cuestión distinta es por qué y para qué, pues es posible demostrar que todo árbol enraizado ordenado es isomorfo a un árbol enraizado diádico[69].



De su recorrido en orden obtenemos la expresión en forma infija

$$(0 + (1 - 2)) \cdot (3^\wedge 5) \cdot ((1/4)^\wedge 5),$$

equivalente aritméticamente a la anterior.

§ 10 De las redes

Pudiésemos decir que una `red` es la representación como grafo (o multigrafo) de un sistema de conexiones entre entidades reales.

La terminología empleada en grafos se traslada a redes. No obstante, existen diferencias, matices y nuevos términos. Por ejemplo, si el grafo que representa la red es pesado hablamos de una `red de enlaces pesados`.

También en la teoría de redes es habitual hablar de `nodos` y `enlaces`, en vez de vértices y aristas. Además, se distinguen y destacan algunos tipos de nodos según la funcionalidad de la red; a modo de ejemplo, en una *red de transporte simple* destacan el `nodo fuente` —sin arcos de entrada— (el nodo de salida), y el `nodo sumidero` —sin arcos de salida— (el nodo de llegada).

Distinguimos entre `red homogénea`, aquélla en la que todos sus nodos tienen un grado similar, y `red heterogénea`, aquélla en la que existen nodos con un grado muy bajo y otros con un grado muy alto. Estos últimos suelen denominarse `nodos superconectores`.

Una característica de las redes en el mundo real es que crecen o decrecen en tamaño. En ellas, puede suceder que cuanto mayor sea el grado de un nodo existente en la red, mayor es la probabilidad de que un nodo nuevo se enlace con él, fenómeno conocido como `enlazamiento preferencial` (o, sinónimamente, `principio de la popularidad atractiva`). Claro que también existen redes en las que la tendencia es que los nodos de grado bajo se enlacen con nodos de grado bajo y los de gra-

[69] *Vid. v. gr.* https://en.wikipedia.org/wiki/Binary_tree#Encoding_general_trees_as_binary_trees.

do alto con los de grado alto (`redes asortativas`), y otras en las que la tendencia es que haya más enlaces entre los nodos de grado bajo y los de grado alto (`redes disasortativas`).

Puede suceder que los nodos enlazados con un mismo nodo estén enlazados entre sí o que no lo estén. Cuando dos de tales nodos no están enlazados entre sí si dice que existe un `agujero estructural`. Cuantos menos agujeros estructurales en torno a un nodo existan, más podremos hablar de `agrupamiento` (*cluster*) en torno a dicho nodo.

Pudiésemos definir una relación de equivalencia en la red, considerando `equivalentes estructuralmente` aquellos nodos que tienen el mismo número y tipo de enlaces (tipo, por ejemplo, en cuanto a un menor o mayor grado, o a menos o más agujeros estructurales).

§ 11 De algunos artefactos: Truth Tree Solver, PSeInt y SageMath

Para algunos de los ejemplos y varias de las actividades estudiamos determinadas realizaciones en varios artefactos en línea, genéricos o específicos, con herramientas o con programas lógico-matemáticos; a modo de ejemplo, The Truth Tree Solver[70], PSeInt[71] y SageMath[72], respectivamente.

The Truth Tree Solver es un artefacto en línea específico de construcción automática de tablas semánticas que usaremos cuando estudiemos éstas[73]; de hecho, allí encontraremos una relación de más artefactos[74].

PSeInt es una herramienta que nos asiste en el aprendizaje de la programación: permite escribir algoritmos en pseudocódigo en español; permite generar el diagrama de GOLDSTINE y NEUMANN (el diagrama de flujo «clásico») y el de NASSI y SHNEIDERMAN; puede traducir el algoritmo en pseudocódigo a C, C++, C#, Java, JavaScript, MatLab, Pascal, PHP, Python 2, Python 3 o QBasic Visual Basic.

SageMath es un programa lógico-matemático del que la misión de su equipo es crear una alternativa viable, libre y abierta a Magma, Maple, Mathematica y Matlab; además, utiliza un amplio abanico de software existente como NumPy, SimPy o Maxima, admitiendo directamente código escrito en otros lenguajes como Sage, Gap[75], GP, HTML, Macaulay2, Maxima, Octave, Python, R o Singular. Acerca de SageMath es posible consultar, en español, por ejemplo, [24] (aportes documentales en español de la comunidad) y [25] (que aunque verse exclusivamente sobre grafos, es muy apropiado para aprender), y en inglés, [26] (aportes documentales de la comunidad) y [27] —original en francés, traducido al alemán y al inglés, que además es conocimiento libre, con licencia Atribución-CompartirIgual 4.0 Internacional[76]—, además de una sucinta bibliografía en estas notas[77]. Es posi-

[70] http://www.formallogic.com/en/truth-tree-solver.
[71] http://pseint.sourceforge.net/.
[72] https://www.sagemath.org/.
[73] *Cfr. infra* § 3.3 (pág. 274 de esta edición).
[74] *Vid. infra* § 3.3.9 (pág. 319 de esta edición).
[75] El lenguaje Gap que interpreta SageMath es propio de GAP (Groups, Algorithms, Programming).
[76] https://creativecommons.org/licenses/by-sa/4.0/deed.es.
[77] *Vid. infra* § 17.19 (pág. 940 de esta edición).

ble realizar la interpretación (ejecución) de los códigos escritos en SageMathCell[78], la celda libre de computación en línea, e incrustable en páginas web, de SageMath, donde una vez escrito el código, pulsando [Evaluate], nos devolverá el resultado. Si bien, si queremos disfrutar de toda la potencia de SageMath es necesaria su instalación[72].

§ 12 Bibliografía

- *Ex ante* (para su lectura y repaso previo por parte del alumnado):
  - En español:

[28] Francisco Javier González Ortiz. Proyecto MATEX, 2004. http://personales.unican.es/gonzaleof/ (accedido el 25.1.2018). ©gratis OA.

[29] Textos Marea Verde. Apuntes Marea Verde, 2024. http://www.apuntesmareaverde.org.es/grupos/mat/index.html (accedido el 26.1.2024). ©CC BY-NC-SA.

  - En inglés:

[30] CK-12 Foundation. K-12 FlexBooks, 2024. https://www.ck12.org/fbbrowse/ (accedido el 26.1.2024). ©CK-12 License.

[31] Siyavula Education. Open Textbooks, 2024. https://www.siyavulaeducation.com/work-oer.html (accedido el 26.1.2024). ©CC BY-ND.

- *In itinere* (para su consulta durante el estudio de la materia):
  - Árboles:

[32] Félix García Merayo. *Matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 2015.

  - SageMath:
    - En español:

[24] Varios. Sage Math Español. https://www.sagemath.org/es/ (accedido el 26.1.2024). ©CC BY-NC-SA.

[25] Ana María Vieites Rodríguez, Felicidad Aguado Martín, Felipe Gago Couso, Manuel Ladra González, Gilberto Pérez Vega y Concepción Vidal Martín. *Teoría de grafos. Ejercicios resueltos y propuestos. Laboratorio con Sage*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2014. http://www.paraninfo.es/-catalogo/9788428337076/teoria-de-grafos–ejercicios-y-problemas-resueltos. ©TDR.

[78] https://sagecell.sagemath.org/.

- En inglés:

[26] SAGE DEVELOPMENT TEAM. *Sage Documentation v10.1*, 2023. https://doc.sagemath.org/html/en/index.html (accedido el 26.1.2024). ©gratis OA.

[27] Paul ZIMMERMANN, Alexandre CASAMAYOU, Nathann COHEN, Guillaume CONNAN, Thierry DUMONT, Laurent FOUSSE, François MALTEY, Matthias MEULIEN, Marc MEZZAROBBA, Clément PERNET, Nicolas M. THIÉRY, Erik BRAY, John CREMONA, Marcelo FORETS, Alexandru GHITZA y Hugh Thomas THOMAS. *Computational Mathematics with SageMath*. Autoedición, Nancy, Francia, 2018. Ediciones en alemán, francés e inglés. https://www.sagemath.org/sagebook/english.html (accedido el 26.1.2024). ©CC BY-SA.

(Más bibliografía sobre SageMath en § 17.19 [pág. 940]).

Parte I

Cimientos: lógica y análisis formal

Cuenta la leyenda que un día Verdad y Mentira se cruzaron.

—Buenos días, dijo Mentira.

—Buenos días, dijo Verdad.

—Bonito día, continuó Mentira. Entonces Verdad fue a comprobar si era verdad. Lo era.

—Hermoso día, dijo Verdad.

—El lago está aún más bello, dijo Mentira con una bonita sonrisa.

Entonces Verdad miró hacia el lago y vio que Mentira decía la verdad y asintió.

Mentira corrió hacia el agua y dijo...

—El agua es aún más hermosa y cálida. ¡Vamos a nadar!

Verdad tocó el agua con los dedos y estaba realmente agradable y cálida.

Entonces Verdad confió en Mentira. Ambas se quitaron la ropa y nadaron tranquilamente.

Un poco más tarde, Mentira salió, se vistió con la ropa de Verdad y se fue.

Verdad, incapaz de ponerse la ropa de Mentira, comenzó a caminar sin ropa y todo el mundo se apartaba al verla desnuda.

Entristecida, abandonada, Verdad se refugió en el fondo de un pozo[79].

Así, desde entonces, la gente prefiere aceptar la Mentira disfrazada de verdad que la Verdad desnuda.

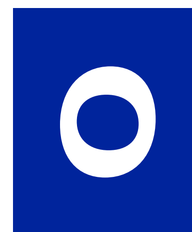
(Autoría desconocida).

---

[79] Hasta que salga y reine —*cfr. v. gr.* https://es.wikipedia.org/wiki/La_verdad_saliendo_del_pozo—. La Verdad, que no una verdad (una creencia fuertemente asentada), ésta no. Pudiésemos leer una selección de trabajos acerca del tema de la verdad en Nicolás y Frápolli [33]. No obstante, debiésemos, pienso, prestarles la atención que merecen: al refrán «Quien no duda, no sabe cosa alguna» (Sevilla y Zurdo [34]), y a los alegatos «*Le doute n'est pas un état bien agréable, mais l'assurance est un état ridicule* [La duda no es un estado muy agradable, pero la seguridad es un estado ridículo]» (Voltaire, Carta a Frédéric Guillaume, príncipe de Prusia, 28 de noviembre de 1770 —*vid. v. gr.* https://books.google.ca/books?id=wDQ-TAAAAQAAJ), «Quien quiera enseñarnos una verdad que no nos la diga: simplemente que aluda a ella con un breve gesto, gesto que inicie en el aire una ideal trayectoria, deslizándonos por la cual lleguemos nosotros mismos hasta los pies de la nueva verdad» (José Ortega y Gasset, *Meditaciones del Quijote*, 1914, p. 80 —*vid. v. gr.* https://archive.org/details/meditacionesdelq00orte—) e «*Insofern sich die Sätze der Mathematik auf die Wirklichkeit beziehen, sind sie nicht sicher, und insofern sie sicher sind, beziehen sie sich nicht auf die Wirklichkeit* [En la medida en que las proposiciones matemáticas se refieren a la realidad, no son ciertas, y en la medida en que son ciertas, no se refieren a la realidad]» (Albert Einstein, *Geometrie and Erfahrung*, 1921 [*vid. v. gr.* https://en.wikiquote.org/wiki/Albert_Einstein]).

Sección A

Lógica matemática



Del lenguaje°

> [...] en la práctica, el pensamiento del matemático no es jamás un pensamiento formalizado: el matemático da un sentido a todas las proposiciones, lo que le permite olvidarse de la expresión de dichas proposiciones dentro de cualquier formalización de la teoría, si es que existe alguna.
>
> (René Thom).

Con este capítulo inicial intentamos ilustrar lo crucial de la elección del tipo de lógica y del lenguaje formal —ambos, aunque incluso cualitativos, definidos— en la representación semántica del conocimiento así como de la traducción inversa, es decir, que nuestros eductos en lenguaje lógico-matemático —una lengua no materna (L1) y no natural, en este caso— correspondan fehacientemente a lo afirmado en nuestra lengua materna (L0) y recíprocamente, la traducción de los aductos en lenguaje lógico-matemático a nuestra lengua materna. Nos limitaremos a representaciones semánticas basadas en la lógica de juntores (caps. 0 a 3), como parte de la lógica de primer orden (caps. 4 y 5), su metalógica (cap. 6), sus estrategias de demostración (cap. 7), sus irregularidades (cap. 8), siguiendo la exposición de algunas de sus extensiones que incluyen nociones no incorporadas en la misma.

° Digamos que me atreví con el prólogo, el preámbulo y los prefacios, pero con éste no osé. Me refiero a que bien pudiese haberlo denominado Prefacio IV o Introducción, a riesgo y ventura de que quien estudie estas notas lo considerase materia primordial y tuviese a bien leerlo, al menos. Sea lo que fuere, su contenido es parte de la basa sostén de los capítulos siguientes; de aquí mi decisión de que no entrase en suerte.

§ 0.0 El concepto

Aunque son ya pocos los textos que distinguen entre concepto y término y juicio y proposición, sería absurdo menospreciar lo esencial de la psicología en el desarrollo de las humanidades y las ciencias[1]. Desde antaño se consideran tres las formas lógicas elementales puramente mentales: el concepto, el juicio y el razonamiento. Veámoslas, y también sus correspondientes aproximaciones como expresiones verbales: el término, la proposición y la argumentación.

Comencemos con el concepto.

§ 0.0.0 De su definición y estructura

La lógica clásica define un *concepto* como la representación mental de una entidad abstracta, de una cosa, sin que se afirme ni niegue nada de ella[2]. La realidad a la que se refiere el concepto la llamamos *objeto* del concepto.

Es costumbre en las obras lingüísticas enmarcar los significados con comillas simples; lo mismo haremos cuando nos refiramos a conceptos para destacar así que aludimos a dicha representación mental.

El concepto, por lo general, posee una *estructura* constituida por partes o *notas conceptuales esenciales*, algunas *constitutivas* y otras *consecutivas* o *derivadas* de las primeras, estructura posiblemente aderezada con otras *notas accidentales*, no esenciales. En cualquier caso, el concepto proviene naturalmente de nuestra actividad mental mientras que su expresión verbal, a la que llamaremos *término*[3],

[1] Por ejemplo, no tenemos más que pensar en John Forbes NASH Jr., la teoría de juegos y la economía.
[2] La *simplex apprehensio rei* —la mera aprehensión de la cosa—.
[3] *Cfr. infra* § 0.3 (pág. 28 de esta edición).

proviene artificialmente de un lenguaje, además, el término es particular para las criaturas humanas que comparten dicho lenguaje, mientras que en este sentido el concepto gozaría de universalidad.

Ejemplo 13

Del concepto de 'número natural':

0., ¿cuáles son sus notas constitutivas?;

1., demos un ejemplo de nota consecutiva/derivada de aquéllas, y

2., demos un ejemplo de nota accidental.

Resolución.— Del concepto de 'número natural':

0. los axiomas de PEANO son sus notas constitutivas;

1. 'infinitos en número' es una nota consecutiva o derivada de aquéllas;

2. 'primo' y 'compuesto' son notas accidentales respecto de la divisibilidad[4]. ■

Llamamos *comprensión* o *intensión* del concepto a la colección de notas o rasgos que lo integran y *extensión* a la colección de entidades concretas que abarca.

§ 0.0.1 De sus clases y relaciones

En cuanto a su comprensión, el concepto se distingue como:

- *simple*, una representación mental de la esencia o naturaleza de su objeto, o
- *compuesto*, en el que en dicha representación mental, a la esencia le acompaña una cualidad.

Ejemplo 14

Demos un ejemplo de cada uno de los conceptos:

0., simple, y

1., compuesto.

Resolución.—

0. 'Hombre' es un concepto simple.

1. 'Científica' es un concepto complejo: 'mujer' y 'profesional de la ciencia'. ■

En cuanto a su extensión, el concepto se distingue como:

[4] En algunos textos se considera que cuando todas las notas accidentales respecto de una misma cualidad o razón se yuxtaponen disyuntivamente conforman una nota consecutiva; en el ejemplo anterior, 'primo o compuesto'.

- *singular*, precisamente si su objeto se reduce a una única entidad, o
- *universal*, precisamente si su objeto es una pluralidad de entidades.

Ejemplo 15

Demos un ejemplo de cada uno de los conceptos:

0., singular, y

1., universal.

Resolución.—

0. 'Tierra' y 'verdad' son conceptos singulares;

1. 'Criatura humana' es un concepto universal. ■

Hablamos de *diversidad entre conceptos* cuando su contenido difiere. Según el monto en que difieran, distinguimos desde *conceptos homogéneos* (o *emparentados*) hasta *conceptos heterogéneos* (o *dispares*), todo ello en menor o mayor grado.

Con respecto a la homogeneidad o emparentamiento, destacamos dos relaciones entre conceptos:

- la *subordinación* entre conceptos se da cuando uno, el *subordinado*, procede del otro, el *subordinante*;
- la *coordinación* entre conceptos ocurre cuando ninguno se deriva del otro, estando subordinados ambos a un tercero.

Estas relaciones de subordinación y coordinación suelen representarse en forma de *árbol enraizado*[5].

Ejemplo 16

Proporcionemos un ejemplo de subordinación y de coordinación entre conceptos.

Resolución.— El concepto de 'número natural' es subordinado al de 'número', coordinado al de 'número entero' y subordinante respecto al de 'número primo'. ■

Con respecto a la heterogeneidad, dividimos los conceptos en:

- *compatibles*, cuando sus objetos pueden coexistir en una misma realidad, e

[5] *Cfr. supra* § 9.0 (pág. xcv de esta edición).

- *incompatibles*, cuando no es posible dicha coexistencia, donde a su vez se distingue entre conceptos:
  - *en oposición contradictoria*, uno representa una realidad y el otro su negación;
  - *en oposición contraria*, de cualidades incompatibles pero pertenecientes a un género común;
  - *en oposición privativa*, uno representa una cualidad y el otro su privación, y
  - *en oposición relativa*, cuyas realidades son términos de una relación determinada.

Ejemplo 17

Deemos un ejemplo de cada uno de los conceptos:

0., compatibles;
1., incompatibles en oposición contradictoria;
2., incompatibles en oposición contraria;
3., incompatibles en oposición privativa, e
4., incompatibles en oposición relativa.

Resolución.—

0. Los conceptos de 'mujer' y 'profesional de la ciencia' son compatibles.
1. Los conceptos de 'ser' y 'nada' son un ejemplo de conceptos en oposición contradictoria.
2. Los conceptos '—2' y '2' están en oposición contraria, pues son incompatibles con respecto a la cualidad de signo, pero pertenecen al género común de número.
3. Los conceptos de 'infinitud' y 'finitud', definida la primera como carencia de la segunda, son conceptos en oposición privativa.
4. Dos conceptos en relación de subordinación están en oposición relativa, por ejemplo 'número natural' y 'número primo'; también lo están dos conceptos cuya relación sea «secuencial», como la de los conceptos 'causa' y 'efecto'. ■

§ 0.1 El juicio

§ 0.1.0 De su definición y clases

De acuerdo con Aristóteles, un *juicio* es una representación mental consistente en la afirmación o negación de algo sobre algo.

Por esto, lo que caracteriza al juicio es su función predicativa, es decir, el afirmar o negar algo sobre algo. Así, las partes materiales del contenido representativo del juicio son dos:

- la representación del objeto, el *sujeto* del juicio, y
- la representación de lo atribuido al sujeto, el *predicado* del juicio.

En definitiva, en el juicio, los conceptos pueden desempeñar el papel de sujeto o de predicado.

Según incluya explícitamente sujeto o predicado y no el otro, el juicio se distingue como existencial o impersonal.

- Un *juicio existencial* es aquél que aparentemente carece de predicado, aunque podría reescribirse con predicado.
- Un *juicio impersonal* es aquél que representa una acción o suceso que, en principio, no puede atribuirse a una entidad determinada, aunque es posible que la causa de tal imposibilidad sea nuestra ignorancia o desconocimiento de quién o qué origina la acción o el suceso, por lo que sí que tendría sujeto.

Ejemplo 18

Demos un ejemplo de cada uno de los juicios

0., existencial, e

1., impersonal.

Resolución.—

0. El juicio ‘se tienen veintitrés situaciones’ es existencial al estar explícito el sujeto y no el predicado; observemos que pudiésemos reescribirlo como ‘las veintitrés situaciones son reales’, siendo ‘las veintitrés situaciones’ el sujeto y ‘son reales’ el predicado.

1. Los juicios ‘se dice’, ‘nieva’ son impersonales por estar explícito el predicado y no el sujeto. ■

Observación 0.1.0.— Suele llamarse *juicio de inherencia* aquél en que al objeto de un concepto le es atribuido o negado algo, sea, por ejemplo, una acción, una cualidad, un modo de ser; entonces, como cualquier característica o relación comparativa de tal objeto puede ser tratada como inhe-

rente a dicho objeto, pudiésemos aceptar que, supuestos los objetos, todo juicio puede reducirse a un *juicio de inherencia* y que, en definitiva, todos los juicios tengan la forma sujeto-predicado defendida por Aristóteles.

Ejemplo 19

Determinemos la forma sujeto-predicado de los juicios:

0., 'la verdad es para ser dicha', y

1., 'el número 3 es el siguiente al número 2'.

Resolución.—

0. En el juicio 'la verdad es para ser dicha', 'la verdad' es sujeto y 'para ser dicha' es predicado.[6]

1. En el juicio 'el número 3 es el siguiente al número 2', que es posible reescribir '$3 = 2 + 1$', el sujeto es 'el número 3', esto es, '3', y el predicado es 'es el siguiente al número 2', esto es, '$= 2 + 1$'. ■

Según su *extensión*, esto es, su *cantidad*, distinguimos entre:

- *juicio universal*, en el que el sujeto actúa en toda su extensión, es decir, el sujeto está tomado universalmente;
- *juicio particular*, en el que el sujeto se toma sólo en una parte de su extensión, o sea, el sujeto está tomado particularmente, y
- *juicio singular*, en el que el sujeto es un objeto singular, a saber, el sujeto está tomado singularmente.

[6] Un análisis actual aproximado diría algo así: oración simple, copulativa, enunciativa y afirmativa, formada por:
- sujeto (sintagma nominal)
  - determinante: la
  - núcleo: verdad
- predicado nominal (sintagma verbal)
  - núcleo copulativo: es
  - atributo (sintagma preposicional)
    - enlace: para
    - término (sintagma nominal)
      - núcleo: ser
      - complemento del núcleo (sintagma adjetival) cuyo núcleo es «dicha».

Ejemplo 20

Demos un ejemplo de cada uno de los juicios:

0., universal;
1., particular, y
2., singular.

Resolución.—

0. 'Todas las verdades son para ser dichas' es un juicio universal.
1. 'Algunas verdades son para ser dichas' es un juicio particular.
2. 'Esta verdad es para ser dicha' es un juicio singular. ■

Según su *comprensión*, esto es, su *cualidad*, distinguimos entre:

- *juicio afirmativo*, (o, sinónimamente, *juicio positivo*), en el que el predicado está incluido en la comprensión del sujeto, es decir, el predicado está tomado partiular o singularmente, sólo en parte de su extensión, y
- *juicio negativo*, en el que el sujeto no incluye en su comprensión al predicado, estando este último tomado universalmente, o sea, en la totalidad de su extensión.

Ejemplo 21

Demos un ejemplo de cada uno de los juicios:

0., afirmativo, y
1., negativo.

Resolución.—

0. 'La verdad es para ser dicha' es un juicio afirmativo.
1. 'La verdad no es para ser dicha' es un juicio negativo. ■

Según la *naturaleza de la unión entre el sujeto y el predicado*, sea un vínculo sencillo o exprese éste una dependencia, suelen dividirse los juicios en categóricos, hipotéticos y disyuntivos.

- Un *juicio categórico* es el que afirma o niega un predicado de un sujeto, una enunciación sin más, en particular sin estar el predicado supeditado a ninguna condición.
- Un *juicio hipotético* (o, sinónimamente, *juicio condicional*), es aquél que la verdad o falsedad de una enunciación, lo condicionado o tesis, depende de la verdad o falsedad de una situación, la condición o hipótesis.

- Un *juicio disyuntivo* es el que enuncia varios predicados, en realidad alternativas, acerca de un sujeto; se sobreentiende que una de ellas es verdadera y las otras falsas, es decir, que se excluyen mutuamente, por lo que la condición se encuentra dentro de la predicación: para que una alternativa sea verdadera es necesario que las otras sean falsas.

Ejemplo 22

Demos un ejemplo de cada uno de los juicios:

0., categórico;
1., hipotético, y
2., disyuntivo.

Resolución.—

0. 'La verdad es para ser dicha' es un juicio categórico. 'No existe el mayor de los números naturales', que es posible reescribir como 'el conjunto de los números naturales no tiene máximo', también es un juicio categórico.
1. 'Si la ética es nuestra guía, la verdad es para ser dicha' es un juicio hipotético.
2. El juicio 'la verdad es para ser dicha, reservada u oculta' es disyuntivo [trabajamos por y para que la primera alternativa ser la verdadera, ¿verdad?]. ■

Observación 0.1.1.— Quizás pudiesen distinguirse más tipos de juicio; por ejemplo, pudiésemos llamar juicios conjuntivos a aquéllos que enuncian simultáneamente varios predicados simples, si bien no sería más que un caso particular de juicio categórico. De hecho, una vez que nos centremos en las expresiones verbales de los juicios, las proposiciones (auténticas), distinguiremos todas las posibles conexiones.

Observación 0.1.2.— Por otra parte, cómo no mencionar en este punto las tres visiones de la estructura de la *norma jurídica* que, según Hans KELSEN, no es más que un juicio hipotético, según Carlos COSSIO, un juicio disyuntivo, y según Eduardo GARCÍA MÁYNEZ, es un juicio categórico o hipotético dependiendo del momento que se considere.

Es de interés una *división metalógica de los juicios según la modalidad*, atendiendo a la cual se dividen en apodícticos, asertóricos y problemáticos.

- Un *juicio apodíctico* es en el que lo enunciado por el predicado respecto del sujeto es incondicionalmente verdadero. Distinguimos, a su vez, los *juicios de necesidad*, en los que dicha relación de predicado a sujeto es inclusiva y los *juicios de imposibilidad* en los que es exclusiva.

- Un *juicio asertórico* enuncia un hecho confirmado. A veces se le denomina *juicio de hecho* (en oposición al juicio de necesidad o imposibilidad) y *juicio contingente* (indicando que podría haber sucedido en forma distinta).
- Un *juicio problemático* enuncia un hecho posible pero aún no confirmado.

Ejemplo 23

Demos un ejemplo de cada uno de los juicios:

0., apodíctico de necesidad;
1., apodíctico de imposibilidad;
2., asertórico, y
3., problemático.

Resolución.—

0. ‘0 es un número’ es un juicio apodíctico de necesidad. El juicio ‘0 no es un número irracional’ es apodíctico de imposibilidad.
1. ‘Eratóstenes calculó el diámetro de la Tierra’ es un juicio asertórico, bien de hecho, ya que puede pensarse una relación distinta —imaginó, trazó, etc.—, bien contingente —porque bien pudo haber sido calculado por otra persona—.
2. ‘Se evitará el enfriamiento del núcleo terrestre’ es un juicio problemático. ■

Finalmente, también es importante la *división epistemológica de los juicios* en analíticos y sintéticos (Immanuel Kant).

- Un *juicio analítico* es aquél en el que la noción del sujeto incluye al predicado.
- Un *juicio sintético* es aquél en el que el predicado constituye un agregado a la noción del sujeto, por ejemplo, una peculiaridad de éste.

Ejemplo 24

Demos un ejemplo de cada uno de los juicios:

0., analítico, y
1., sintético.

Resolución.—

0. ‘El conjunto vacío es el conjunto sin elementos’ es un juicio analítico.
1. ‘0 es el elemento neutro de la suma entre números enteros’ es un juicio sintético. ■

§ 0.1.1 De su relación por oposición

Decimos que dos juicios son *heterogéneos* (o, sinónimamente, *diversos*), cuando no coinciden en sujeto o predicado; *homogéneos*, en caso contrario.

Decimos que dos juicios son *opuestos* precisamente si siendo homogéneos lo que enuncian es distinto.

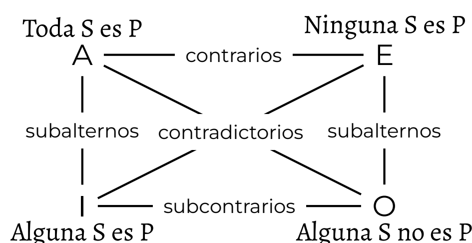
Dos juicios opuestos lo son *en cualidad* precisamente si uno de ellos es afirmativo y el otro negativo, esto es, que de un mismo sujeto, un mismo predicado sea en uno afirmado y negado en el otro.

Dos juicios opuestos lo son *en cantidad* precisamente si uno de ellos es universal y el otro particular, es decir, que de un mismo sujeto, un mismo predicado afirme o niegue universalmente en uno y particularmente en el otro.

Los juicios se relacionan *por oposición* de tres formas:

- *oposición contradictoria* es la que media entre juicios que se oponen tanto en cualidad como en cantidad; son parejas de juicios en oposición contradictoria,
  - AO, formada por el *juicio universal afirmativo* (A) y el *juicio particular negativo* (O), y
  - EI, formada por el *juicio universal negativo* (E) y el *juicio particular afirmativo* (I);
- *oposición contraria* es la que media entre juicios universales que se oponen en cualidad; es pareja de juicios en oposición contraria,
  - AE, formada por el *juicio universal afirmativo* (A) y el *juicio universal negativo* (E);
- *oposición subcontraria* es la que media entre juicios particulares que se oponen en cualidad; es pareja de juicios en oposición subcontraria,
  - IO, formada por el *juicio particular afirmativo* (I) y el *juicio particular negativo* (O);
- *oposición de subalternación* es la que media entre juicios que se oponen en cantidad; son parejas de juicios en oposición de subalternación,
  - AI, formada por el *juicio universal afirmativo* (A) y el *juicio particular afirmativo* (I), y
  - EO, formada por el *juicio universal negativo* (E) y el *juicio particular negativo* (O).

Estas interrelaciones suelen representarse mediante el que se conoce como *cuadro de oposición*:



Ejemplo 25

Proporcionemos ejemplos de parejas de juicios AO, EI, AE, IO, AI y EO, comentando sus relaciones de oposición.

Resolución.—

0. AO son contradictorios, y EI, también; es decir, A y O se oponen tanto en cualidad (universal frente a particular) como en cantidad (afirmativo frente a negativo); similar oposición sucede entre E e I; por ejemplo:

   - «todas las verdades son para ser dichas» (A) frente a «algunas verdades no son para ser dichas» (O);
   - «ninguna verdad es para ser dicha» (E) frente a «alguna verdad es para ser dicha» (I);

1. AE son contrarios, esto es, A y E son juicios universales que se oponen en cualidad (afirmativo frente a negativo); por ejemplo:

   - «todas las verdades son para ser dichas» (A) frente a «ninguna verdad es para ser dicha» (E);

2. IO son subcontrarios, esto es, I y O son juicios particulares que se oponen en cualidad (afirmativo frente a negativo); por ejemplo:

   - «alguna verdad es para ser dicha» (I) frente a «algunas verdades no son para ser dichas» (O);

3. AI están en relación de subalternancia, y EO, también, esto es, A e I se oponen en cantidad (universal frente a particular); similar oposición sucede entre E y O; a los universales, A y E, los llamamos *subalternantes*; a los particulares, I y O, los llamamos *subalternados* (o, sinónimamente, *juicios subalternos*)—; por ejemplo:

   - «todas las verdades son para ser dichas» (A) frente a «alguna verdad es para ser dicha» (I);
   - «ninguna verdad es para ser dicha» (E) frente a «algunas verdades no son para ser dichas» (O). ■

Observación 0.1.3.— Un enunciado popular de la paremia relacionada con los ejemplos anteriores es «No todas las verdades son para ser dichas»[7].

[7] *Vid. v. gr.* SEVILLA y ZURDO [34].

§ 0.1.2 De la verdad y falsedad por oposición

La verdad y falsedad de los juicios cuando éstos se relacionan por oposición se expresa de la siguiente forma, dependiendo de la forma de dicha oposición.

Oposición contradictoria

Sucede de dos juicios contradictorios que no pueden ser ambos verdaderos, de donde si uno es verdadero, su contradictorio es falso.

. . . .

Dado que hemos avanzado el lenguaje lógico-matemático en § 52 (pág. lxxvi de esta edición) y a falta de presentarlo en profundidad en § 0.7 (pág. 49 de esta edición), § 4.0 (pág. 365 de esta edición) y capítulos posteriores, comenzamos a utilizarlo para familiarizarnos con él.

. . . .

Teorema 0.0

Se satisface:

0. $A \to \neg O$;
1. $O \to \neg A$;
2. $E \to \neg I$;
3. $I \to \neg E$.

Ejemplo 26

Proporcionemos un ejemplo para cada una de las afirmaciones de este teorema.

Resolución.— Dos juicios contradictorios, no pueden ser ambos verdaderos; por ejemplo:

0. $A \to \neg O$: si es verdad que «de noche, todos los gatos son pardos», entonces es falso que «de noche, algún gato no es pardo»;
1. $O \to \neg A$: si es verdad que «de noche, algún gato no es pardo», entonces es falso que «de noche, todos los gatos son pardos»;
2. $E \to \neg I$: si es verdad que «nadie escarmienta en cabeza ajena», entonces es falso que «alguien escarmienta en cabeza ajena»;
3. $I \to \neg E$: si es verdad que «alguien escarmienta en cabeza ajena», entonces es falso que «nadie escarmienta en cabeza ajena». ■

Tampoco dos juicios contradictorios pueden ser ambos falsos, de donde si uno es falso, su contradictorio es verdadero.

Teorema 0.1
Se satisface:
0. $\neg A \to O$;
1. $\neg O \to A$;
2. $\neg E \to I$;
3. $\neg I \to E$.

Ejemplo 27

Proporcionemos algún ejemplo para cada una de las afirmaciones de este teorema.

Resolución.— Dos juicios contradictorios, no pueden ser ambos falsos; por ejemplo:

0. $\neg A \to O$: si es falso que «todas [las personas] escarmientan en cabeza ajena», entonces es verdad que «alguien no escarmienta en cabeza ajena»;
1. $\neg O \to A$: si es falso que «de noche, algún gato no es pardo», entonces es verdad que «de noche, todos los gatos son pardos»;
2. $\neg E \to I$: si es falso que «de noche, ningún gato es pardo», entonces es verdad que «de noche, algún gato es pardo»;
3. $\neg I \to E$: si es falso que «alguien escarmienta en cabeza ajena», entonces es verdad que «nadie escarmienta en cabeza ajena». ■

Oposición contraria

Sucede de dos juicios contrarios que no pueden ser ambos verdaderos, de donde si uno es verdadero, su contrario es falso.

Teorema 0.2
Se satisface:
0. $\neg(A \wedge E)$,

y, por lo tanto:
1. $A \to \neg E$;
2. $E \to \neg A$.

Ejemplo 28

Proporcionemos un ejemplo para cada una de las afirmaciones de este teorema.

Resolución.— Dos juicios contrarios no pueden ser ambos verdaderos, por ejemplo,

0. $\neg(A \wedge E)$: no puede suceder que sea verdad que «de noche, todos los gatos son pardos» y que también sea verdad que «de noche, ningún gato es pardo»;

lo que sí sucede es que si uno es verdadero, su contrario es falso:

1. $A \to \neg E$: si es verdad que «de noche, todos los gatos son pardos», entonces es falso que «de noche, ningún gato es pardo»;
2. $E \to \neg A$: si es verdad que «nadie escarmienta en cabeza ajena», entonces es falso que «todas [las personas] escarmientan en cabeza ajena». ■

Teorema 0.3
Dos juicios contrarios pueden ser ambos falsos.

Ejemplo 29

Proporcionemos un ejemplo de dos juicios falsos y contrarios.

Resolución.— En efecto, dos juicios contrarios pueden ser ambols falsos, por ejemplo,

- $\neg A \wedge \neg E$: puede suceder que sea falso que «de noche, todos los gatos son pardos» y que también sea falso que «de noche, ningún gato es pardo» [como de hecho así es, ni ninguno ni todos son pardos, sólo algunos]. ■

Actividad 0.0
Propongamos un ejemplo que corrobore que dado un juicio universal falso, su contrario puede ser verdadero o falso.

Oposición subcontraria

Sucede de dos juicios subcontrarios no pueden ser ambos falsos, de donde si uno es falso su subcontrario es verdadero:

Teorema 0.4

Se satisface que

0. $\neg(\neg I \wedge \neg O)$,

y, por lo tanto:

1. $\neg I \to O$;
2. $\neg O \to I$.

Ejemplo 30

Proporcionemos un ejemplo para cada una de las afirmaciones de este teorema.

Resolución.— Dos juicios subcontrarios no pueden ser ambos falsos:

0. $\neg(\neg I \wedge \neg O)$: un par de ejemplos:
   - no puede suceder que sea falso que «alguien escarmienta en cabeza ajena» y que también sea falso que «alguien no escarmienta en cabeza ajena»;
   - no puede suceder que sea falso que «de noche, algún gato es pardo» y que también sea falso que «de noche, algún gato no es pardo»;

lo que sí sucede es que si uno es verdadero, su subcontrario es falso:

1. $\neg I \to O$: si es falso que «alguien escarmienta en cabeza ajena», entonces es verdad que «alguien no escarmienta en cabeza ajena»;
2. $\neg O \to I$: si es falso que «de noche, algún gato no es pardo», entonces es verdad que «de noche, algún gato es pardo». ■

Teorema 0.5

Dos sucesos subcontrarios pueden ser ambos verdaderos.

Ejemplo 31

Proporcionemos dos ejemplos de dos juicios verdaderos y subcontrarios.

Resolución.—

0. $I \wedge O$: puede suceder que sea verdad que «alguien escarmienta en cabeza ajena» y que también sea verdad que «alguien no escarmienta en cabeza ajena»;
1. $I \wedge O$: puede suceder que sea verdad que «de noche, algún gato es pardo» y que también sea verdad que «de noche, algún gato no es pardo». ■

Actividad 0.1

Propongamos un ejemplo que corrobore que dado un juicio particular verdadero, su subcontrario puede ser verdadero o falso.

Oposición de subalternación

Teorema 0.6

La verdad del juicio universal implica la verdad del particular, es decir:

0. $A \rightarrow I$;
1. $E \rightarrow O$.

Ejemplo 32

Proporcionemos un ejemplo para cada una de las afirmaciones de este teorema.

Resolución.—

0. $A \rightarrow I$: si es verdad que «de noche, todos los gatos son pardos», entonces es verdad que «de noche, algún gato es pardo»;

1. $E \rightarrow O$: si es verdad que «nadie escarmienta en cabeza ajena», entonces es verdad que «alguien no escarmienta en cabeza ajena». ■

Teorema 0.7

La falsedad del universal no implica la falsedad del particular, esto es:

0. $\neg A \nrightarrow \neg I$;
1. $\neg E \nrightarrow \neg O$.

Ejemplo 33

Proporcionemos un ejemplo para cada una de las afirmaciones de este teorema.

Resolución.—

0. $\neg A \nrightarrow \neg I$: la falsedad del universal «toda persona es buena» no implica la falsedad del particular «alguna persona es buena» (pues, de hecho, hay personas buenas);

1. $\neg E \nrightarrow \neg O$: la falsedad del universal «ninguna persona es buena» no implica la falsedad del particular «alguna persona no es buena» (efectivamente, hay personas que no son buenas). ■

Teorema 0.8
La falsedad del particular conlleva la falsedad del universal, esto es:
0. $\neg I \to \neg A$;
1. $\neg O \to \neg E$.

Ejemplo 34

Proporcionemos un ejemplo para cada una de las afirmaciones de este teorema.

Resolución.—
0. $\neg I \to \neg A$: si es falso que «alguna persona tiene páginas», entonces es falso que «toda persona tiene páginas»;
1. $\neg O \to \neg E$: si es falso que «alguna persona no es buena», entonces es falso que «ninguna persona es buena». ■

Teorema 0.9
La verdad del particular no implica la verdad del universal, es decir:
0. $I \nrightarrow A$;
1. $O \nrightarrow E$.

Ejemplo 35

Proporcionemos un ejemplo para cada una de las afirmaciones de este teorema.

Resolución.—
0. $I \nrightarrow A$: la verdad de «de noche, algún gato es pardo» no implica la verdad de «de noche, todos los gatos son pardos»;
1. $O \nrightarrow E$: la verdad de «alguien no escarmienta en cabeza ajena» no implica la verdad de «nadie escarmienta en cabeza ajena». ■

§ 0.1.3 De su relación por implicación y por equivalencia

Como la experiencia con lo anterior nos dicta, decimos que un primer juicio *implica* un segundo juicio cuando, y sólo cuando, el sentido, valor y significación del primero validen el sentido, valor y significación del segundo.

Por otra parte, los juicios se relacionan por equivalencia precisamente si tienen igual sentido, igual valor, igual significación; se dirá de ellos que son *juicios equivalentes* (*aequipollent*).

Ejemplo 36

Proporcionemos dos juicios en relación de implicación y dos equivalentes.

Resolución.— El juicio 'toda verdad es para ser dicha' implica el juicio 'hay una verdad que es para ser dicha'. Los juicios 'toda verdad es para ser dicha' y 'no hay ninguna verdad que no sea para ser dicha' son equivalentes. ■

En el ejemplo 196 (pág. 380 de esta edición) vemos los juicios del ejemplo anterior como proposiciones y también su equivalencia, en la lógica de primer orden.

§ 0.1.4 De su relación por conversión

Los juicios se relacionan *por conversión* de tres formas:

- *conversión simple* (*simpliciter convertitur*), la que sucede cuando se intercambian sujeto y predicado sin alterar ni la cualidad ni la cantidad del juicio; la admiten los juicios universales negativos (E) y los particulares afirmativos (I), en el sentido de que sólo para estos juicios se da la equivalencia entre el juicio original y su converso simple;
- *conversión accidental* (*per accidens*), la que sucede cuando además de intercambiar sujeto y predicado se altera la cantidad al particularizar lo universal; la admiten los juicios universales afirmativos (A) y negativos (E), en el sentido de que, sólo para estos juicios sucede que el juicio original implica su converso accidental;
- *conversión por contraposición* (*per contra*: *sic fit conversio tota*), la que sucede cuando además de intercambiar sujeto y predicado se altera la cualidad; la admiten los juicios universales afirmativos (A) y los particulares negativos (O), en el sentido de que sólo para estos juicios se da la equivalencia entre el juicio original y su converso por contraposición.

Ejemplo 37

Proporcionemos ejemplos de juicios relacionados por conversión, para cada forma y cada juicio admitido por la forma.

Resolución.—

0. De conversión simple:
    - de 'ninguna verdad es para ser dicha' (E) obtenemos por conversión simple 'nada de lo que es para ser dicho es verdad' (E), ambos equivalentes;

- de 'alguna verdad es para ser dicha' (I) obtenemos por conversión simple 'algo de lo que es para ser dicho es verdad' (I), ambos equivalentes;

1. De conversión accidental:

   - de 'toda verdad es para ser dicha' (A) obtenemos por conversión accidental 'algo de lo que es para ser dicho es verdad' (I), el primero implicando el segundo (suponiendo que existe algo de lo que es para ser dicho);

   - de 'ninguna verdad es para ser dicha' (E) obtenemos por conversión accidental 'algo de lo que es para ser dicho no es verdad' (I), el primero implicando el segundo (suponiendo que existe algo de lo que es para ser dicho);

2. De conversión por contraposición:

   - de 'toda verdad es para ser dicha' (A) obtenemos su juicio contrapuesto 'todo lo que no es para ser dicho no es verdad' (A), ambos equivalentes;

   - de 'alguna verdad no es para ser dicha' (O) obtenemos su juicio contrapuesto 'algo de lo que no es para ser dicho es verdad (no es una no verdad)' (O), ambos equivalentes. ■

§ 0.1.5 De su relación por obversión

Los juicios se relacionan *por obversión* precisamente si los sujetos son los mismos, los predicados son contradictorios (uno es P y el otro, $\neg P$) y son opuestos en cualidad (uno es afirmativo y el otro negativo). La obversión es válida para los cuatro tipo de juicios A, E, I y O, en el sentido de que se da la equivalencia entre el juicio original y su obverso.

Ejemplo 38

Proporcionemos ejemplos de juicios relacionados por obversión, para cada tipo.

Resolución.—

0. De 'toda verdad es para ser dicha' (A) obtenemos su juicio obverso 'ninguna verdad es para no ser dicha' (E), ambos equivalentes;

1. de 'ninguna verdad es para ser dicha' (E) obtenemos su juicio obverso 'toda verdad es para no ser dicha' (A), ambos equivalentes;

2. de 'alguna verdad es para ser dicha' (I) obtenemos su juicio obverso 'alguna verdad no es para no ser dicha' (O), ambos equivalentes;

3. de 'alguna verdad no es para ser dicha' (O) obtenemos su juicio obverso 'alguna verdad es para no ser dicha' (I), ambos equivalentes. ■

§ 0.1.6 De disyuntivo a categórico pasando por hipotético

Mediando esta relación de equivalencia, es posible transformar un juicio disyuntivo en uno categórico vía su transformación primera en uno hipotético.

Ejemplo 39

Transformemos en categóricos los juicios disyuntivos ‘el agua está en movimiento o en calma’, ‘septiembre, o lleva los puentes, o seca las fuentes’ y ‘o no todo quieres o todo perderás’.

Resolución.— Los juicios disyuntivos:

- ‘el agua está en movimiento o en calma’,
- ‘septiembre, o lleva los puentes, o seca las fuentes’[8],
- ‘o no todo quieres o todo perderás’,

se transforman en sus equivalentes hipotéticos:

- ‘si el agua no está en movimiento, entonces está en calma’,
- ‘septiembre, si no lleva los puentes, seca las fuentes’,
- ‘si todo quieres, todo perderás’,

y finalmente en sus equivalentes categóricos:

- ‘el agua está en calma en caso de no estar en movimiento’,
- ‘septiembre, seca las fuentes en caso de que no lleve los puentes’,
- ‘todo perderás en caso de que todo quieras’. ■

§ 0.1.7 Transformaciones por negación entre opuestos

Mediante sencillas «operaciones», en realidad con la negación, es posible transformar un juicio en otro equivalente a su opuesto. Tres son las transformaciones correspondientes: transformación de A en su opuesto contradictorio O (*prae contradic*); transformación de A en su opuesto contrario E (*post contra*), y transformación de I en su opuesto subalternante A (*prae-post-que subalter*).

[8] Es disyuntivo en el sentido de que ambas cosas no pueden suceder simultáneamente (aunque sí a lo largo de la extensión del mismo septiembre).

Ejemplo 40

Siendo A «toda verdad es para ser dicha», E «ninguna verdad es para ser dicha», I «alguna verdad es para ser dicha» y O «alguna verdad no es para ser dicha», ejemplifiquemos las transformaciones

0., *prae contradic*;

1., *post contra*, y

2., *prae-post-que subalter*.

Resolución.—

0. Transformación *prae contradic*: de «toda verdad es para ser dicha» (A) obtenemos «no toda verdad es para ser dicha» que es equivalente a «alguna verdad no es para ser dicha» (O); observemos que se ha negado el universal.

1. Transformación *post contra*: de «toda verdad es para ser dicha» (A) obtenemos «toda verdad no es para ser dicha» que es equivalente a «ninguna verdad es para ser dicha» (E); observemos que se ha negado lo afirmado.

2. Transformación *prae-post-que subalter*: de «alguna verdad es para ser dicha» (I) obtenemos «no hay verdad que no sea para ser dicha» que es equivalente a «toda verdad es para ser dicha» (A); observemos que se ha negado simultáneamente el existencial y lo afirmado. ■

Para el caso de la subcontrariedad, con la negación no es posible, esto es, en el ejemplo precedente, de «alguna verdad es para ser dicha» (I), ¿qué juicio obtendríamos que fuese equivalente a «alguna verdad no es para ser dicha» (O)?

En el ejemplo 195 (pág. 379 de esta edición) vemos las transformaciones de los juicios del ejemplo anterior como transformaciones entre proposiciones de la lógica de primer orden; en dicho ejemplo también nos formulamos la pregunta sobre la subcontrariedad en esta lógica.

§ 0.2 El razonamiento

§ 0.2.0 De su definición y estructura

Definición 0.0.— El *razonamiento* es aquella representación mental en que un juicio se nos presenta en conexión necesaria con otro u otros de los cuales se deriva.

Un razonamiento se descompone en juicios: el *antecedente* del razonamiento consta de uno o más juicios de los que se deriva el *consiguiente* o *conclusión* del razonamiento, el juicio derivado, que se obtiene por necesidad de los del antecedente.

§ 0.2.1 De sus clases

Distinguimos entre razonamiento:

- *inmediato*, caso de que el antecedente conste de un único juicio, y
- *mediato*, caso de que el antecedente conste de una pluralidad de juicios, distinguiéndose entre:
  - *deductivo*, en cuyo antecedente hay un juicio universal y cuya conclusión es un juicio particular, que a su vez se subdivide en:
    - *categórico*, en cuyo antecedente y conclusión sólo hay juicios categóricos;
    - *hipotético*, en cuyo antecedente hay un juicio hipotético y cuya conclusión suele ser un juicio categórico, y
    - *disyuntivo*, en cuyo antecedente hay un juicio disyuntivo y cuya conclusión suele ser un juicio categórico.
  - *inductivo*, en cuyo antecedente hay juicios particulares o singulares y cuya conclusión es un juicio universal,
  - *por analogía*, que de juicios particulares concluye un juicio particular, y
  - *con ejemplos*, a veces partícipes éstos de una inducción como los casos singulares de los que parte —ejemplos *reveladores* de una verdad general—, otras muy parecida a la analogía —ejemplos *ilustrativos* de una verdad general—.

Ejemplo 41

Proporcionemos ejemplos de razonamientos para cada una de las clases anteriores.

Resolución.—

0. Este razonamiento es inmediato:

‘Los números enteros son números racionales’.

Luego: ‘Un número que no es racional no es un número entero’.

1. Este razonamiento es (mediato deductivo) categórico:

‘La verdad es para ser dicha’.

‘Esta conclusión no es para ser dicha’.

Luego: ‘Esta conclusión no es verdad’.

2. Este razonamiento es (mediato deductivo) hipotético, en *modalidad positiva*:

‘Si la ética es nuestra guía, la verdad es para ser dicha’.

‘La ética es nuestra guía’.

Luego: ‘La verdad es para ser dicha’.

y éste lo es en *modalidad negativa*:

‘Si nuestro grado ético baja, la maldad sube’.

‘La maldad no sube’.

Luego: ‘Nuestro grado ético no baja’.

3. Este razonamiento es (mediato deductivo) disyuntivo, en *modalidad positivo-negativa*:

‘La verdad es para ser dicha, reservada u oculta’.

‘Esta verdad es para ser dicha’.

Luego: ‘Esta verdad no es para ser reservada ni para ser oculta’.

y éste lo es en *modalidad negativo-positiva*:

‘La verdad es para ser dicha, reservada u oculta’.

‘Esta verdad no es para ser reservada ni para ser oculta’.

Luego: ‘Esta verdad es para ser dicha’.

4. Este razonamiento es (mediato) inductivo:

‘Dadas las condiciones X, en los sucesos A, B, C, etc., se ha observado el mismo fenómeno Y’.

‘El fenómeno Y es indicio de una verdad general en las condiciones X’.

Luego: ‘En los sucesos A, B, C, etc., se ha descubierto una verdad general en las condiciones X’.

‘Las verdades generales en las condiciones X permanecen válidas siempre que no cambien dichas condiciones X’.

Luego: ‘La verdad general que genera los sucesos A, B, C, etc., seguirá así por siempre (es universal) (en las condiciones X)’.

Por ejemplo: como estos gatos [A, B, C, etc.] los hemos observado de noche [condiciones X] y todos estos gatos son pardos [fenómeno Y], entonces [inducimos] que de noche [condiciones X], todos los gatos —sin excepción— son pardos [ésta es la verdad general en las condiciones X].

5. Este razonamiento es (mediato) por analogía:

'La entidad *A* tiene la propiedad *P*'.

'La entidad *A* posee la característica *C*'.

Luego: 'Todas las entidades que posean la característica *C* tienen la propiedad *P*'.

[Hasta aquí, una inducción (incorrecta)].

'La entidad *B* posee la característica *C*'.

Luego: 'La entidad *B* tiene la propiedad *P*'.

[Esto último ha sido una deducción (correcta)]. 

A la expresión verbal del razonamiento (mediato deductivo) categórico la llamamos *silogismo*[9].

En § 5.7 (pág. 432 de esta edición), repasaremos alguna de estas clases de razonamiento y estudiaremos alguna más; por el camino, estudiaremos varias técnicas y estrategias para demostrar la validez o invalidez de un razonamiento.

§ 0.3 Expresión verbal del concepto: el término

Definición 0.1.— Un *término* (o, sinónimamente, *signo lingüístico*), es una unidad mínima lingüística, una palabra o colección de palabras, que expresa un sentido, conocimiento o idea, en definitiva, que expresa un concepto, por ejemplo, «número» o «cualquier número natural es mayor o igual que cero».

Definición 0.2.— El *significante* de un signo lingüístico es la hilera de grafías que lo componen o en el caso hablado, la hilera de sonidos (la imagen gráfica/visual o la imagen acústica, respectivamente); por ejemplo, en el caso de «número», seis letras, una con tilde, del alfabeto español; es la extensión física del signo, también se conoce como su *expresión*.

Definición 0.3.— El *significado* —también llamado *significación*, *acepción* o *contenido*— de un signo lingüístico es la representación mental asociada al significante, esto es, el *concepto* que representa este último —la idea de número en el ejemplo con el que comenzamos este subcapítulo—.

Quienes participan en un proceso de comunicación, por ejemplo, en un acto de habla, comparten un *código*, que no es otra cosa que lo que enlaza los significantes con sus significados en el sistema de significación en el que están usando los signos.

Suelen clasificarse los términos,

[9] *Cfr. infra* § 5.0 (pág. 399 de esta edición).

- respecto de la *polisemia* y *sinonimia*, en:
  - *unívocos*, también llamados *monosignificativos*, aquéllos que poseen una única significación;
  - *multívocos*, también llamados *polisignificativos* o *polisémicos*, que poseen una pluralidad de significaciones, y suele distinguirse en éstos entre una *acepción primaria* y *acepciones secundarias*, y
  - decimos que dos términos son *términos sinónimos* precisamente si siendo distintos corresponden a un mismo concepto.
- respecto de su *independencia*, en:
  - *categoremáticos*, con significado por sí mismos, y
  - *sincategoremáticos*, con significado sólo cuando acompañan a los anteriores.
- respecto de su *universalidad*, en:
  - *concretos*, que designan una peculiaridad de un sujeto particular, y
  - *abstractos*, que designan una peculiaridad de un sujeto genérico.
- respecto de su *aplicabilidad*, en:
  - *distributivos*, aplicable a todas las entidades de la pluralidad que designa, y
  - *colectivos*, no aplicable a ninguna de las entidades de la pluralidad que designa.

Ejemplo 42

Proporcionemos ejemplos de términos para cada una de las clases anteriores.

Resolución.—

0. El término «conjunto de los números primos» es unívoco.
1. Los términos «árbol», «raíz», «hoja» son polisémicos, todos con una acepción primaria, la referida a la naturaleza y con una acepción secundaria matemática.
2. Los términos «árbol diádico» y «árbol binario» son sinónimos.
3. El término «número primo» es categoremático, mientras que «algunos», «todos», «bastantes», «sólo dos», «ninguno», son términos sincategoremáticos.
4. Los términos «necio», «asociativo», «conmutativo» son concretos, mientras que «necedad», «asociatividad», «conmutatividad», son términos abstractos.
5. El término «número primo» es distributivo, mientras que «conjunto de los números primos» es un término colectivo. ■

En el lenguaje ordinario y en el lógico-matemático, el término presenta varias propiedades, entre ellas las de apelación y suposición (*suppositio*):

- un término tiene la propiedad de *apelación* precisamente si es posible su aplicación a otro término;
- la propiedad de *suposición* se refiere al uso del término en lugar del concepto, del objeto o de la palabra, y se distingue entre:
  - *suposición real* —ocurre con frecuencia en el lenguaje ordinario—, que sucede precisamente si se usa el término en lugar del objeto y no del concepto ni de la palabra;
  - *suposición material* —ocurre con frecuencia en lingüística—, que sucede precisamente si se usa el término en lugar de la palabra y no del concepto ni del objeto, y
  - *suposición formal* —ocurre con frecuencia en el lenguaje lógico-matemático—, que sucede precisamente si se usa el término en lugar del concepto y no del objeto ni de la palabra.

Ejemplo 43

Para las propiedades de apelación y de suposición, propongamos ejemplos de términos que las presenten.

Resolución.—

0. El término «conmutativo» tiene la propiedad de apelación; por ejemplo, en «$(\mathbb{N};+)$ es conmutativo», el término «conmutativo» (término *apelante*) se aplica al término «$(\mathbb{N};+)$» (término *apelado*).
1. En «esta taza es tuya», el término «taza» supone el objeto (una taza real —esta taza—) y no el concepto ni la palabra (suposición real).
2. En «“número primo” es una expresión verbal escrita que consta de dos palabras», el término «número primo» supone esas dos palabras (representamos mentalmente ambas palabras conformando dicha expresión verbal) y no el concepto ni el objeto (suposición material).
3. En «todo número primo es mayor que uno», el término «número primo» supone un concepto, el de número primo, y no el objeto ni la palabra (suposición formal). ■

El estudio de los términos, su adopción preferente frente a los conceptos y la de las formas verbales frente a las formas lógicas —mentales—, abocó en la línea innovadora de investigación y desarrollo en la lógica medieval, la *lógica terminista*. Esta lógica centra su estudio en la validez de las inferencias, lo más formal posible. Y así hasta nuestros días.

§ 0.4 Expresión verbal del juicio: la proposición

§ 0.4.0 Oración declarativa, enunciado y frase

Manteniendo por juicio la definición anterior, esto es, una representación mental consistente en la afirmación o negación de algo sobre algo, admitimos la siguiente de oración declarativa como expresión verbal de un juicio —si bien, la proposición, como más adelante se desprenderá sin esfuerzo, la envolverá— y sus emparentadas de oración, enunciado y frase.

Definición 0.4.— Una *oración* (o, sinónimamente, *sentencia*), es una secuencia significativa de signos lingüísticos.

Definición 0.5.— Una *oración declarativa* (o, sinónimamente, *oración enunciativa* u *oración aseverativa*), es una oración compuesta por un sujeto y un verbo, cuya significación comporta siempre una pretensión de verdad o falsedad, de afirmar o negar algo, pretensión que constituye el valor lógico de la oración declarativa[10].

Esta pretensión de afirmación o negación, la expresamos mediante una *relación lógica* entre conceptos mediante la que afirmamos o negamos uno del otro. De aquí que una oración declarativa sea la *expresión verbal* de un juicio[11].

Así, la oración declarativa es al juicio más o menos lo que el término al concepto.

Definición 0.6.— Un *enunciado* (o, sinónimamente, *expresión declarativa*), es una unidad mínima comunicativa con sentido completo pragmático, posiblemente dependiente de factores contextuales.

Un enunciado puede ser una palabra o una secuencia de palabras; en cualquier caso, insistimos, es una oración declarativa o una parte de una oración declarativa en algún contexto, y como tal, tiene valor de verdad en dicho contexto.

Ejemplo 44

Mostremos que «múltiplo de 12» es una oración declarativa en un contexto determinado.

[10] Una oración tiene sentido, aunque puede carecer de valor de verdad; la existencia de este último caracteriza la oración declarativa.
[11] Como expresión verbal de un juicio, pudiésemos distinguir entre su *expresión oral* y su *expresión escrita*, la primera quizás más natural en el sentido de obedecer a reglas menos rígidas.

Resolución.— En efecto, la expresión «múltiplo de 12» es un enunciado que es una oración declarativa en un contexto determinado, esto es, para un sujeto y verbo concretos; por ejemplo, para el sujeto «36» y el verbo «ser», la expresión verbal «36 es múltiplo de 12» corresponde al juicio '36 es múltiplo de 12' —concepción puramente mental—. ■

Observación 0.4.0.— Es cada vez más frecuente el uso de 'oración declarativa' y 'enunciado' —que se sobreentiende contextualizado— como sinónimos.

Definición 0.7.— La colección de palabras componentes de un enunciado se denomina *frase*.

§ 0.4.1 La proposición

Llegamos en este punto a la concreción de la representación verbal equivalente a un juicio —representación puramente mental—, la proposición.

Definición 0.8.— Una *proposición* (o, sinónimamente, *proposición auténtica* o *proposición enunciativa*), es una clase de equivalencia de oraciones declarativas equivalentes lógicamente, es decir, semánticamente.

Una proposición se presenta así como el *contenido semántico* de cualquier oración declarativa o enunciado contextualizado que la expresa.

Un concepto, varios términos: términos sinónimos. Un juicio, varias oraciones declarativas; todas ellas con la misma significación, el mismo juicio. Un juicio, una proposición. Así, el juicio es a la proposición aproximadamente lo que el concepto a la colección de términos sinónimos correspondiente.

Es por englobar la proposición a la oración declarativa, por lo que también decimos de la proposición que es la expresión verbal del juicio.

Ejemplo 45

Proporcionemos ejemplos de oraciones declarativas equivalentes lógica y semánticamente a «12 divide a 36».

Resolución.— Oraciones declarativas equivalentes lógica y semánticamente a «12 divide a 36» son, por ejemplo, «12 es divisor de 36», «12 es un factor de 36», «12 es un submúltiplo de 36», $12 \mid 36$, «existe un número natural k tal que $36 = 12 \cdot k$», «36 es divisible por 12», «36 es múltiplo de 12, «$36 = \dot{12}$». Todas ellas pertenecen a la misma clase de equivalencia —proposición auténtica—, sirviendo

cualquiera de ellas como representante de dicha clase, por ejemplo,

$$\begin{aligned}[12 \text{ divide a } 36] = [12 \text{ es divisor de } 36] = \cdots = [36 = \dot{12}] \\ = \{&12 \text{ divide a } 36, \\ &12 \text{ es divisor de } 36, \\ &12 \text{ es un factor de } 36, \\ &12 \text{ es un submúltiplo de } 36, \\ &12 \mid 36, \\ &\text{existe un número natural } k \text{ tal que } 36 = 12 \cdot k, \\ &36 \text{ es divisible por } 12, \\ &36 \text{ es múltiplo de } 12, \\ &36 = \dot{12}, \\ &\ldots\}.\end{aligned}$$ ■

Observación 0.4.1.— De aquí en adelante designaremos la proposición sin los corchetes indicadores de clase de equivalencia, esto es, mediante cualquiera de sus representantes.

Ejemplo 46

Proporcionemos un ejemplo de:

0. una proposición;
1. una proposición verdadera;
2. una proposición falsa, y
3. una oración que no sea proposición.

Resolución.—

0. «Esta bola es verde» es una proposición, pues si la bola es verde es verdadera y si es de otro color, falsa.
1. «Esta frase es verdadera» es una proposición verdadera.
2. «Esta bola roja es verde» es una proposición falsa.
3. «Esta frase es falsa» no es una proposición, pues si es cierta entonces es falsa, y si es falsa, entonces es cierta. ■

Observación 0.4.2.— En el lenguaje ordinario es frecuente utilizar sinonímicamente los nombres oración declarativa, proposición, enunciado, juicio y frase. ¡Cuidado con ello! No es lo mismo el lenguaje ordinario que el lenguaje lógico-matemático.

§ 0.4.2 Sujeto, predicado y su representación

Aunque pudiésemos continuar la exposición en términos de los juicios —representaciones puramente mentales—, preferimos trabajar de aquí en adelante con sus expresiones verbales, las proposiciones. En otras palabras, hacemos una suposición formal, empleamos proposición en vez de juicio (análogamente a la suposición formal de término en lugar de concepto[12].

De acuerdo con la lógica aristotélica, una proposición se representa esquemáticamente por «S es P» siendo el sujeto (S), la cópula («es») y el predicado (P) las tres componentes constituyentes de la proposición. De hecho, en una lengua humana natural, la mayoría de las expresiones declarativas constan de un sujeto y un predicado.

Definición 0.9.— *Grosso modo*,

- el *sujeto* es la parte de la proposición que representa una entidad o noción acerca de la cual la proposición afirma o niega algo, y
- el *predicado* es la parte de la proposición que representa lo que se afirma o niega del sujeto, una *peculiaridad* —una propiedad o una no-propiedad, en menor o mayor grado— del sujeto[13].

Según afecte sólo a una, dos, tres, cuatro..., o más entidades, decimos que es, respectivamente, un *predicado monádico* (o, sinónimamente, *predicado absoluto*), *diádico*, *triádico*, *tetrádico*..., o un *predicado poliádico* (o, sinónimamente, *predicado relativo*).

Para representar entidades concretas utilizaremos las primeras letras minúsculas latinas a, b, c, d..., anotadas o no por subíndices, a_0, a_1..., que llamaremos *constantes individuales*. Para representar entidades arbitrarias utilizaremos las últimas letras minúsculas latinas x, y, z, anotadas o no por subíndices, x_0, x_1..., que llamaremos *variables individuales*. Para cada variable debería conocerse la clase de entidades a la que representa, su *rango* (o, sinónimamente, su *universo de discurso*, *dominio* o *micromundo*). De cada entidad que pertenece a la clase representada por una variable decimos que es un *valor* o *instancia* de dicha variable. Para representar predicados utilizaremos las letras mayúsculas latinas P, Q, R..., anotadas o no por subíndices, P_0, P_1..., que llamaremos *letras predicativas*.

Con respecto al orden de constituyentes en la proposición, son frecuentes tres notaciones para los predicados diádicos en función de la posición de la letra predicativa respecto de las variables o constantes:

- *prefija*: Pxy o $P(x, y)$,

[12] *Cfr. supra* pág. 30 de esta edición.

[13] En la construcción —análisis, diseño, implementación, implantación y explotación— de sistemas informáticos se utiliza el *análisis entidad-relación* (Chen[35]). En este análisis se distingue entre *entidades* —cosas distinguibles—, *relaciones* —interacciones entre entidades— y *atributos* —propiedades de las entidades y relaciones— (*cfr. v. gr.* Hawryszkiewycz [36] (págs. 110ss.) [acerca de la persona, *Vid. v. gr.* https://en.wikipedia.org/wiki/Igor_Hawryszkiewycz]).

- *infija*: xPy,
- *sufija o postfija*: xyP o $(x, y)P$,

siendo la primera la habitual para las funciones —P como función—, la segunda para las relaciones —P es una relación y vía ella, x está relacionado con y, por ejemplo, $x \leq y$— y operaciones —P es una operación y vía ella, x opera con y, por ejemplo, $x + y$— y estructural —por ejemplo, «x e y son P»—[14].

Para el caso de un predicado poliádico y $k + 1$ entidades, $x_0, x_1, \ldots, x_k$, la notación es similar:

- *prefija*: $Px_0x_1 \ldots x_k$ o $P(x_0, x_1, \ldots, x_k)$,
- *infija*[15]: $x_0Px_1P \cdots Px_k$, y
- *postfija*: $x_0x_1 \ldots x_kP$ o $(x_0, x_1, \ldots, x_k)P$.

Ejemplo 47

Formalicemos la proposición «36 es múltiplo de 12» en notación prefija.

Resolución.— En la proposición «36 es múltiplo de 12», identificamos

- el predicado diádico «ser múltiplo de» que designamos por Pxy, y
- dos entidades, 36 y 12,

tras lo que conviniendo en las representaciones:

$a_0 \fallingdotseq 36$,

$a_1 \fallingdotseq 12$,

$P \fallingdotseq$ ser múltiplo de,

pudiésemos formalizar dicha proposición en notación prefija:

$$Pa_0a_1.$$

■

§ 0.4.3 Proposiciones categóricas

En el apartado anterior hemos tratado precisamente con las que se conocen como proposiciones categóricas, las proposiciones de la lógica aristotélica.

[14] No quisiésemos que se nos olvidase mencionar la *teoría autopoiética* y cómo en ella se distingue en un sistema entre su *organización* —«conjunto de propiedades relacionales de los componentes»— y su *estructura* —«conjunto de propiedades materiales contingentes respecto de la organización»— (*vid.* Fernández Ostalaza y Moreno Bergareche [37], págs. 31ss.).

[15] Un ejemplo notable de notación prefija es la *notación polaca* —*vid.* actividad 1.21 (pág. 174 de esta edición)—.

Definición 0.10.— Una *proposición categórica* es aquélla que afirma o niega que un sujeto satisface un predicado, esto es, esquemáticamente, S es P.

Como decíamos, el sujeto puede ser singular o plural, esto es, puede haber uno o varios sujetos y esto hace que se hable de *predicados monádicos*, también llamados *singulares* o *unitarios*, que son aquéllos que representan una afirmación o negación acerca de un solo sujeto —por ejemplo, «x es un número» (un único sujeto: x)—, *diádicos*, también llamados *binarios*, que representan una afirmación o negación sobre dos sujetos —por ejemplo, «x es un número menor o igual que 1» (dos sujetos: x y 1)—, *triádicos*, también llamados *ternarios* —por ejemplo, «x es un número mayor o igual que 0 y menor o igual que 1» (tres sujetos: x, 0 y 1)—, y así sucesivamente.

Observación 0.4.3.— La x que hemos usado en los ejemplos anteriores es una *variable lógica* y 0 y 1 son instancias de dicha variable, esto es, constantes.

Aristóteles clasificó las proposiciones categóricas atendiendo no sólo a la *cualidad*, según sean afirmativas o negativas, sino también a la *cantidad*, esto es, teniendo en cuenta si el sujeto se toma universal, particular o singularmente, es decir, si se consideraban todas, algunas o una concreta de las entidades del *universo* —que también llamaremos *ámbito/contexto/dominio/región/territorio* (*de discurso/de interpretación/de referencia*) o *referencial*— que lo circunscriba. De esta manera, distinguió cuatro naturalezas básicas en ellas, A, I, afirmativas, y E, O, negativas:

- *proposiciones categóricas afirmativas*:

  A: toda x es y; (*universal afirmativa*)

  I: alguna x es y; (*particular afirmativa*)

- *proposiciones categóricas negativas*:

  E: ninguna x es y; (*universal negativa*)

  O: alguna x no es y. (*particular negativa*)

Consideró, además, la concreción a entidades (*términos singulares*):

a es y; (*singular afirmativa*)

a no es y. (*singular negativa*)

Observación 0.4.4.— Para Aristóteles, la formalización lógica de cualquier expresión verbal tenía la estructura S es P. Es importante saber que para él, las partículas «todo», «ningún», «algún» eran sujetos de predicación en una proposición. No será hasta 1879 cuando Friedrich Ludwig Gottlob Frege considera los cuantores como entidades lógicamente independientes[16].

[16] *Cfr. infra* § 4 (pág. 364 de esta edición).

Observación 0.4.5.— Recordemos en este punto lo estudiado en el subcapítulo § 0.1 (pág. 9 de esta edición), en concreto, en el apartado § 0.1.1 (pág. 14 de esta edición) y siguientes.

Observación 0.4.6.— Las figuras 0.0, 0.2 y 0.1 (págs. respectivas 37, 39 y 38, de esta edición) muestran la representación diagramática de A, I, E y O, con diagramas de LEIBNIZ[17] y EULER[18], diagramas de CARROLL[19] y diagramas (lógicos) de VENN[20], respectivamente.

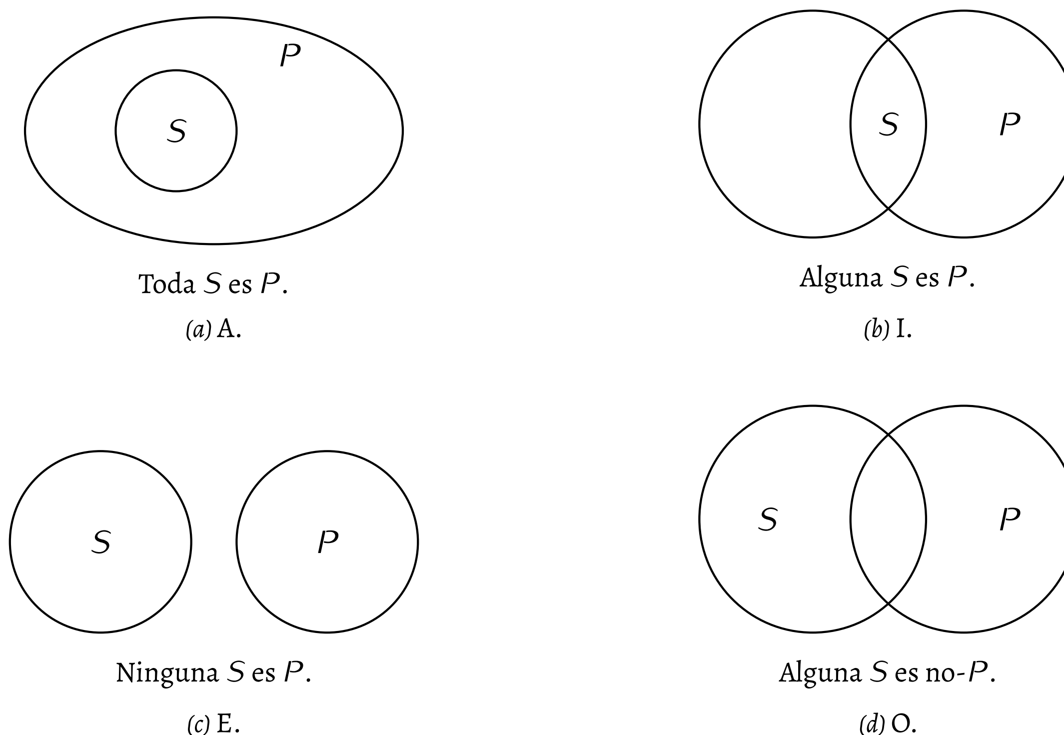


Figura 0.0.— Representación con diagramas de LEIBNIZ y EULER de las proposiciones categóricas A, I, E y O.

[17] *Cfr.* LEIBNIZ, *New Essay comparing human understanding*, 1704.
[18] *Cfr.* EULER, *Lettres à une Princesse d'Allemagne*, 1768.
[19] *Vid.* CARROLL, *The Game of Logic*, 1886.
[20] *Vid.* VENN, *Symbolic Logic*, 1881.

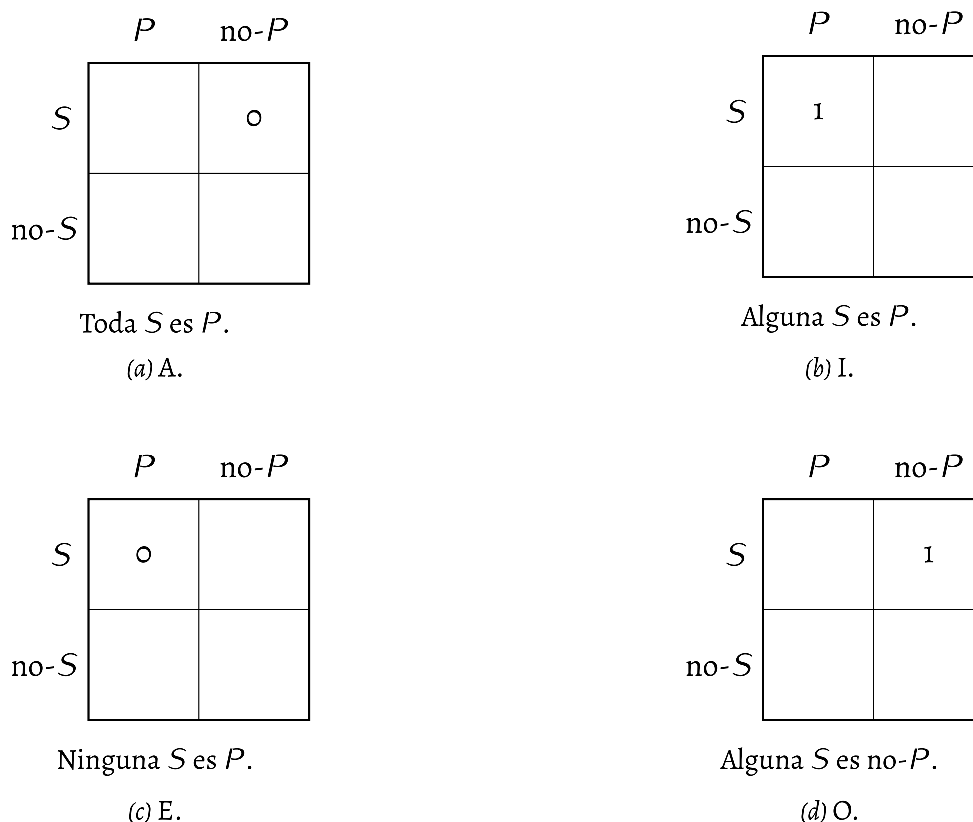


Figura 0.1.— Representación con diagramas de CARROLL de las proposiciones categóricas A, I, E y O. Comenzando por la superior izquierda y siguiendo el movimiento de las manecillas del reloj, las cuadrículas representan: S y P, S y no-P, no-S y no-P, y no-S y P; una cuadrícula con un 0 designa que no existen entidades que la satisfagan; una con un 1 designa la existencia de entidades que la satisfacen; una cuadrícula en blanco designa que no sabemos si existen o no entidades que la satisfacen.

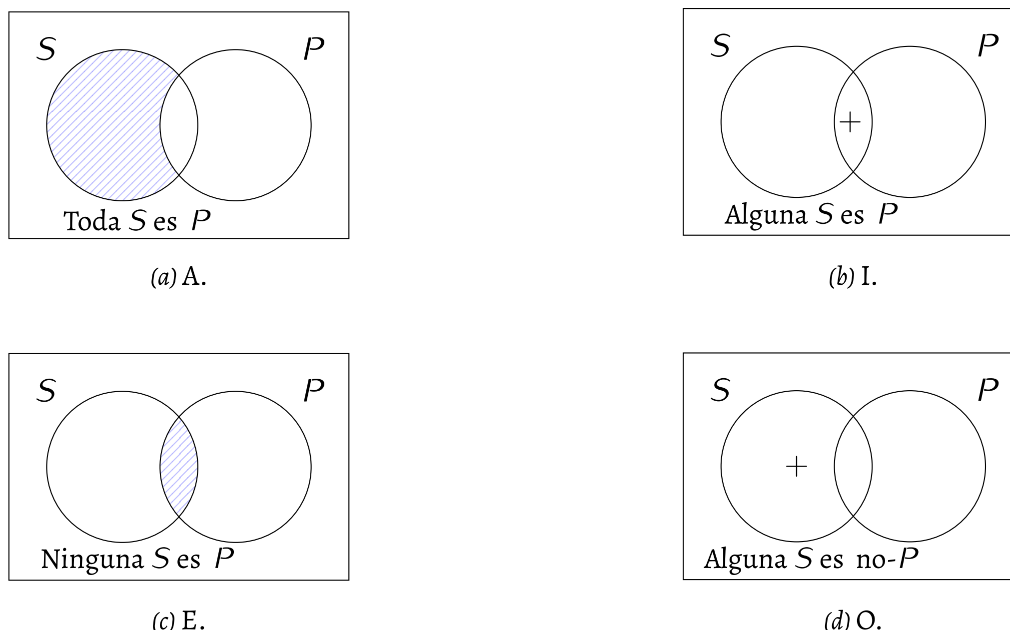


Figura 0.2.— Representación con diagramas de VENN de las proposiciones categóricas A, I, E y O. Un área rayada designa que no hay entidades en ella, que está vacía; un área con el signo + designa la existencia de entidades en el área, esto es, que no está vacía; un área blanca designa que no sabemos si está vacía o no.

Observación 0.4.7.— Anticipándonos a la lógica de primer orden (LPO) y a la lógica de clases (LC), si bien con apoyo en los preliminares vistos en el Prefacio III[21], tenemos la siguiente relación.

Categóricas	Español	LPO	LC
Universal afirmativa (A)	Todo S es P.	$\forall x(Sx \to Px)$	$S \subseteq P$
Existencial afirmativa (I)	Algún S es P.	$\exists x(Sx \land Px)$	$S \cap P \neq \emptyset$
Universal negativa (E)	Ningún S es P.	$\forall x(Sx \to \neg Px)$	$S \cap P = \emptyset$
Existencial negativa (O)	Algún S no es P.	$\exists x(Sx \land \neg Px)$	$S \setminus P \neq \emptyset$

§ 0.4.4 Principios lógicos

Tres son los principios generales que propuso la lógica tradicional y que siguen formando parte de la lógica bivalente de primer orden. Son:

0.°, *Principio de la identidad*: toda proposición se identifica consigo misma;

1.°, *Principio de la no contradicción*: ninguna proposición puede ser afirmada y negada a la vez, y

2.°, *Principio del tercio excluso*: toda proposición debe ser afirmada o negada.

Observación 0.4.8.— Otras lógicas puede que no acepten estos principios.

[21] *Vid. supra* § 52 (pág. lxxvi de esta edición).

> *The law of excluded middle is true when precise symbols are employed, but it is not true when symbols are vague, as, in fact, all symbols are* [La ley del tercero excluido es cierta cuando se emplean símbolos precisos, pero no es cierta cuando los símbolos son vagos, como, de hecho, lo son todos los símbolos]. (Bertrand RUSSELL, Vagueness, *The Australasian Journal of Psychology and Philosophy*, 1923 [Vol. 1, págs. 84–92]).

En efecto, soslayando *pro tempore* esta observación de RUSSELL, el principio del tercio excluso no se satisface cuando consideramos más de dos posibilidades. Así ocurriría, por ejemplo, si quisiésemos formalizar lógicamente una encuesta cuyas respuestas fuesen «sí», «no», «no sabe (o no contesta)», pudiésemos para ello usar la *lógica trivalente*; de manera similar, si quisiésemos formalizar lógicamente un proceso de votación que incluye las posibilidades «voto a favor», «voto en contra», «voto en blanco» y «voto nulo», pudiésemos acudir a la *lógica tetravalente*.

§ 0.4.5 La coordinación: proposiciones simples y compuestas

Definición 0.11.— Una *proposición simple* (o, sinónimamente, *proposición atómica*) es aquélla que no puede dividirse en proposiciones más pequeñas.

Definición 0.12.— Una *proposición compuesta* (o, sinónimamente, *proposición molecular*) es aquélla que es combinación de varias proposiciones simples, enlazadas entre sí mediante *enlaces extraproposicionales* —o extraoracionales en el caso de oraciones—, esto es poseyendo una *estructura sintáctica coordinada*[22].

Ejemplo 48

La proposición «hoy es miércoles y mañana viernes» es una proposición (auténtica) compuesta.

Resolución.— En efecto, está compuesta por dos: «hoy es miércoles» y «mañana es viernes», enlazadas por la partícula «y». Parece que esta proposición debería ser falsa, pues, independientemente del día en que la consideremos, al menos una de ellas es falsa. Si bien pudiésemos argumentar que podría depender del ámbito semántico, es decir, de los significados acordados, imaginemos que sólo estamos hablando de días de trabajo y el jueves es fiesta, entonces, en efecto, hoy, día de trabajo, es miércoles y mañana, el siguiente día de trabajo, es viernes. Dicho de otro modo, conocer el contexto en el que se interpreta, es decir, en el que se determina su significado, es esencial para poder evaluar la veracidad de una proposición. ■

[22] A primeras, pudiésemos concebir esta estructura sintáctica coordinada como una estructura «superficial» en oposición a las estructuras algebraicas que estudiaremos más adelante (*cfr. infra* § 17 [pág. 834 de esta edición]), sin embargo, estudiaremos que no es así, pues tiene la estructura algebraica de *álgebra de Boole* (*cfr. infra* § 3.7 [pág. 353 de esta edición]).

Representamos las proposiciones por *variables semánticas* que designaremos por letras latinas mayúsculas en itálica A, B, C, etc., afectadas o no por subíndices, A_0, A_1, etc.

Estas composiciones suceden de dos formas básicas, que aquí sólo pincelaremos y más adelante analizaremos:

0.ª, por conexión mediante *juntores*, también llamados *conectores* o *conectivas*[23], ejemplos de los cuales son el *negador* («no A»), el *disyuntor* («A o B o ambas») y el *conjuntor* («A y B»), juntores que se representan formalmente por *signos sentenciales conectivos*, que en el caso de los tres anteriores son $\neg$, $\vee$ y $\wedge$, quedando, pues, $\neg A$, $A \vee B$ y $A \wedge B$, respectivamente, siendo éstas sus *formas lógicas*[24] correspondientes.

1.ª, por anexión de *cuantores*, también llamados *cuantificadores*[25], en cuyo caso interesa distinguir entre proposiciones *particulares* y *generales*, ejemplos de los cuales son el *particularizador* («al menos uno») y el *generalizador* («todos»), que en lenguaje lógico-matemático se representan formalmente por *signos sentenciales cuantificativos*, que en el caso de los dos anteriores son $\exists$ y $\forall$, respectivamente.

Ejemplo 49

La composición que muestra la proposición «hoy es miércoles y mañana viernes», ¿lo es por conexión o por anexión?

Resolución.— Por conexión. En efecto, si A es «hoy es miércoles» y B es «mañana es viernes», la proposición compuesta del ejemplo anterior es

$$A \text{ y } B. \qquad \blacksquare$$

Del estudio de las primeras formas de composición se encarga la *lógica de juntores*, también llamada *lógica de conectores*, *lógica de conectivas*, *lógica proposicional*, *lógica de proposiciones* o *lógica de enunciados*[26]; de las segundas, la *lógica de cuantores*, también llamada *lógica de cuantificadores*, *lógica predicativa*, *lógica de términos* o *lógica de predicados*[27]. Como el estudio de las segundas incluye el de las primeras, a la lógica de cuantores se la conoce como *lógica de primer orden* o *lógica de cuantores/cuantificadores de primer orden* o, a veces, simplemente —y confusamente— como *lógica elemental*. Es la lógica de primer orden un capítulo inicial de la *lógica formal*, la que, por su tratamiento simbólico actual, suele tam-

[23] *Vid. infra* § 1.3 (pág. 77 de esta edición).
[24] *Vid. infra* definición 0.22 (pág. 49 de esta edición).
[25] *Vid. infra* § 4.1.2 (pág. 375 de esta edición).
[26] Debemos tener cuidado con la expresión «lógica de enunciados» pues son muchos los textos en los que por enunciado se entiende una proposición simple o compuesta y tanto lo sea ésta por conexión de juntores como por anexión de cuantores.
[27] También debemos tener cuidado con la expresión «lógica de predicados» ya que, como hemos dicho, entendemos por predicado la colección de palabras de una proposición que representa lo que se afirma o niega del sujeto.

bién llamarse *lógica simbólica*, y concretamente cuando centra su interés, como es nuestro caso, en su aplicación a cuestiones matemáticas, *lógica matemática*.

§ 0.4.6 Proposiciones hipotéticas y disyuntivas

La lógica medieval consideró, además de las categóricas, las proposiciones hipotéticas y las disyuntivas.

Definición 0.13.— Una *proposición hipotética* (también llamada *proposición condicional*), es aquélla que afirma o niega un hecho condicionado; en su forma general, tanto la *proposición condicionante*, la condición, como la *proposición condicionada*, el hecho condicionado, son proposiciones categóricas, esto es, esquemáticamente,

si R es Q, entonces S es P.

Definición 0.14.— Una *proposición disyuntiva* (también llamada *proposición excluyente*) es aquélla que afirma o niega del sujeto uno o más predicados que se excluyen mutuamente, esto es, esquemáticamente,

S es P o Q (y no ambos).

§ 0.4.7 Argumentos de enunciado y funtores

En las expresiones declarativas (enunciados) distinguimos funtores y argumentos de enunciado (participantes seleccionados por un funtor).

Definición 0.15.— Un *argumento de un enunciado* es una expresión que puede o necesita ser esclarecida o incluso determinada.

Definición 0.16.— Un *funtor* es una expresión aclaratoria o determinadora de uno o más argumentos de enunciado.

Un funtor puede anotarse con un subíndice que indique el número de sus argumentos de enunciado. Dicho número puede indicarse, redundantemente, mediante lugares vacíos, señalados mediante letras, llamadas *variables*, en contraposición a aquellas otras letras que representan entidades concretas, denominadas *constantes*.

Ejemplo 50

Expresemos la expresión declarativa «estos dos números son mayores que 0» como un funtor de dos variables.

Resolución.— En la expresión declarativa —que si bien parece pretenderse que sea una proposición, aún es incompleta e imprecisa—,

estos dos números son mayores que 0;

distinguimos, a su vez, la expresión «estos dos números», en la que parece necesario esclarecer cuáles son tales números, y la expresión «son mayores que 0» que, en este ejemplo, si bien aclara no determina, pues existen infinitos números que satisfacen lo expresado por el funtor.

El esquema o forma descompositiva o estructural de esta expresión declarativa es:

$$\{\text{son mayores que } 0\}_2(\text{este número})(\text{este otro número}),$$

que, a su vez, es posible expresar, por ejemplo, con lugares vacíos por argumentos de enunciado,

$$\{\text{son mayores que } 0\}_2(\ )(\ ),$$

o con variables por argumentos de enunciado,

$$\{\text{son mayores que } 0\}_2(x)(y),$$

quedando, en definitiva, como un funtor de dos variables. ■

Ejemplo 51

La expresión declarativa «este número y el 2 son mayores que 0», ¿pudiésemos representarla con una variable y una constante?

Resolución.— Sí:

$$\{\text{son mayores que } 0\}_2(x)(2).$$ ■

Algo similar podría hacerse con el funtor; por ejemplo, un esquema con variables por funtor y por argumentos de enunciado es

$$\{f\}(x)(y).$$

Observación 0.4.9.— Este esquema de variables por funtor y por argumentos de enunciado se asemeja a la notación elemental para la definición de una función, la correspondiente a este ejemplo sería una de dos variables, $f(x, y)$; de hecho hablaremos de *función proposicional*[28].

Notemos también que cuando todos los lugares vacíos y todos los provistos de variables se llenan o sustituyen con argumentos de enunciado, la expresión declarativa se convierte en oración declarativa y por tanto en proposición, al quedar completada y precisada, y poder determinar

[28] *Cfr. infra* § 1.2 (pág. 75 de esta edición).

su verdad o falsedad. Por ejemplo, $\{\text{son mayores que } 0\}_2(0)(1)$, falsa, y $\{\text{son mayores que } 0\}_2(1)(2)$, verdadera. Trataremos esto en mayor profundidad cuando estudiemos la semántica.

Ejemplo 52

Expresemos la expresión declarativa del silogismo hipotético de la lógica de primer orden, «Si toda x es y y toda y es z, entonces toda x es z» como un funtor de tres variables.

Resolución.— La estructura constructiva del silogismo hipotético podría expresarse, por ejemplo, así:

$$\{\text{Si _ entonces _}\}_2(\{\text{_ y _}\}_2(\{\text{toda _ es _}\}_2(x)(y))(\{\text{toda _ es _}\}_2(y)(z)))(\{\text{toda _ es _}\}_2(x)(z)),$$

en esta ocasión incluyendo en el funtor, además del número de argumentos de enunciado, su posición, lo cual complica, seguramente en exceso, la notación. ■

§ 0.4.8 Facetas de la proposición

En la proposición pueden distinguirse dos facetas:

0. la una, vista desde la lógica de juntores, como una expresión declarativa en sí (sintaxis), con un valor lógico (semántica) y una posible relación descriptiva o explicativa, una teoría del significado, con la realidad o mundo posible, con las personas que usan la lengua y los contextos (pragmática[29]);

1. la otra, vista desde la lógica de clases[30], como una composición estructurada.

La verdad de las proposiciones obtenidas por la lógica y las matemáticas, a las que llamaremos *proposiciones formales* o *teoremas*, no depende de los hechos. La verdad de las proposiciones obtenidas por otras ciencias y humanidades —física, química, biología, historia, sociología, etc.— y por la filosofía, a las que llamaremos *proposiciones informativas*, depende de la experiencia sensible, nuestra como humanos y de nuestra tecnología y en último lugar de lo que acontece, de los hechos.

Para poder hablar de la veracidad o falsedad de una expresión declarativa, es decir, de que sea proposición, dicha expresión debe tener significado. El significado y la verdad tautológica de las proposiciones formales es consecuencia de una demostración formal. Sin embargo, para una proposición informativa, ha de establecerse su significado y verificarse su verdad. ¿Cómo? Sigue siendo un problema abierto.

[29] *Cfr. v. gr.* Reyes [38].
[30] *Vid. infra* § 10 (pág. 526 de esta edición).

§ 0.5 Expresión verbal del razonamiento: la argumentación

Definición 0.17.— Una *argumentación* es un encadenamiento de oraciones declarativas en el que la colección de unas primeras justifica una última; como tal, es la expresión verbal de un razonamiento.

En efecto, llamamos argumentación a la expresión verbal de un razonamiento, si bien no existe un nombre comúnmente aceptado y suele usarse el mismo nombre de razonamiento para designar tanto el proceso puramente mental como su expresión verbal. Una denominación alternativa para dicha expresión verbal, quizás más centrada en la conclusión, es *inferencia*.

Pero el lenguaje es ambiguo; además, es mucho lo que, aunque no se exprese, se interpreta tácitamente. De ahí que las argumentaciones, a veces, queden alejadas del lenguaje lógico-matemático. Un estadio intermedio es el argumento.

Definición 0.18.— Un *argumento* es lo expresado por una argumentación en un lenguaje y estructura más cercanos a la lógica-matemática; un argumento suele expresarse como un encadenamiento de proposiciones en el que la colección de unas primeras —*premisas* (también llamadas *hipótesis*)— justifica una última —*conclusión* (también llamada *tesis*)—[31].

Definición 0.19.— Un *esquema argumental* es el correlato de un argumento en lenguaje lógico-matemático, habitualmente en su variante más natural[32].

Ejemplo 53

Sea la argumentación: «Esta persona no tiene el pelo rizado y se sabe que la persona que diseñó el plan tiene el pelo rizado; total, que esta persona no diseñó el plan». Hallemos el argumento correspondiente y la formalización (variables proposicionales, esquema argumental y forma lógica.

[Cubit 2].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Esta persona no tiene el pelo rizado. Si esta persona es la que diseñó el plan, entonces tiene el pelo rizado. Luego, esta persona no diseñó el plan.

[31] La argumentación y el argumento deben ser equivalentes semánticamente. De hecho, asegurar dicha equivalencia es el escollo primario en la formalización. A falta de conocer un algoritmo automático eficiente para determinar la equivalencia semántica entre dos oraciones declarativas en español, un camino es la reescritura y nuestro convencimiento. Debemos razonar reescribiendo la argumentación para intentar aclarar su significado y su estructura, su descomposición en premisas simples y conclusión, acercando a la vez lo afirmado a patrones más sencillos de traducción a la lógica de juntores. La búsqueda de este acercamiento, en definitiva, es la esencia de la conformación del argumento.

[32] *Cfr. supra* pág. lxx de esta edición.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales*:

     Siendo el universo de discurso el conjunto de todas las personas, las variables proposicionales son:

     $A \leftrightharpoons$ Esta persona tiene el pelo rizado;

     $B \leftrightharpoons$ Esta persona diseña el plan.

   - *Esquema argumental*:

     Se tiene $\neg A$.
     Si se supone B, se sigue A.
     ∴ Se sigue $\neg B$.

     que también podría expresarse mediante la *coordinación de proposiciones*

     si C y D, entonces E,

     donde:

     $C \leftrightharpoons$ Sucede que se tiene $\neg A$;

     $D \leftrightharpoons$ Sucede que si se supone B, se sigue A;

     $E \leftrightharpoons$ Sucede que se sigue $\neg B$.

   - *Forma lógica*.

     Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{\neg A, B \to A\}$ y la conclusión ψ, a saber, $\neg B$.

     La fórmula en lógica de juntores que hemos hallado para $\mathcal{A}$, su forma lógica[33], es

     $$\neg A \wedge (B \to A) \to \neg B.$$



§ 0.6 Representación del conocimiento y lógica

Parece poco discutible que el aprendizaje humano —responsable, sin duda, de su evolución y progreso y de su involución y retroceso— está fuertemente influenciado por el conocimiento previo poseído. Los sistemas de *representación de conocimiento* prestan una ayuda empírica razonable a los estudios sobre cambio conceptual, al permitir simular las interferencias que se producen entre los conocimientos nuevos con los que se poseían de antemano, así como el proceso de desarrollo y evolución conceptual.

[33] *Vid. infra* definición 0.22 (pág. 49 de esta edición).

Como formalismo de representación del conocimiento, o sea, como la forma en la que el conocimiento se describe para un grado determinado de *abstracción*, elegimos un formalismo basado en el *lenguaje*[34].

Ejemplo 54

Sea el universo $U = \{0, 1, 2, 3\}$. Eligiendo como lenguaje el sistema binario (sistema de numeración en el que los números se representan con dos cifras, 0 y 1), ¿cómo pudiésemos representar la ocurrencia de las entidades de dicho universo en la reunión $A = \{2, 3\}$?

Resolución.— *Grosso modo*, sin entrar en más formalismos, utilizando sólo dos entidades de $\mathcal{U}$, mediante el cuarteto[35] 0011, ya que sus bits[36], leídos de izquierda a derecha, representarían el conocimiento siguiente: el primer 0, que 0 no está en A; el segundo 0, que 1 no está en A; el primer 1, que 2 está en A, y el segundo 1, que 3 está en A. ■

Ejemplo 55

¿Y si fuese a futuro y supiésemos que la entidad 0 sí estará presente, la 1 está en duda, y no estarán ni la 2 ni la 3?

Resolución.— Pudiésemos utilizar una nueva asociación de signos. Por ejemplo, eligiendo como lenguaje el sistema ternario[37]. La palabra ternaria 1200, al ser sus *trits* leídos de izquierda a derecha, representarían el conocimiento siguiente: el 1, que 0 estará en la reunión; el 2, que la 1 está en duda; el primer 0, que 2 no estará, y el segundo 0, que 3 no estará. ■

Según lo presentado y discutido en artículos anteriores, pudiésemos concretar que para que un lenguaje de representación del conocimiento pueda considerarse una *lógica*, debería tener al menos las siguientes características:

[34] Además de lo dicho en el subcapítulo preliminar dedicado a los alfabetos y lenguajes —*vid. supra* § 7 (pág. lxxxv de esta edición)—, pensemos en «otros» lenguajes, por ejemplo, la *notación Laban* (https://en.wikipedia.org/wiki/Labanotation), un sistema de notación del movimiento del cuerpo creado por Rudolf LABAN, ampliamente utilizada en danza —*vid. v. gr.* HUTCHINSON[39]—, la *notación siteswap*, utilizada para describir patrones malabarísticos (https://es.wikipedia.org/wiki/Siteswap), o el *Lenguaje de Expresión de Derechos* o REL (*Rights Expression Language*), un lenguaje procesable por máquina que se utiliza para expresar los derechos de propiedad intelectual —como el derecho de autoría— y otras condiciones de uso sobre el contenido (https://en.wikipedia.org/wiki/Rights_Expression_Language).

[35] Un cuarteto es una palabra binaria de cuatro bits (*nibble*, en inglés). Las posiciones son 3210 (esto se debe a la expresión polinómica del número). La palabra binaria de ocho bits se llama *octeto* (*byte*, en inglés). Un octeto lo conforman dos cuartetos, el de los bits en las posiciones 0 — 3 (*cuarteto inferior*) y el de las posiciones 4 — 7 (*cuarteto superior*).

[36] Dígito binario o bitio (bit, como inglesismo) —en teoría de la información, la unidad de información es el *shannon*, que es la cantidad de información contenida en un bit (equivalentemente, la cantidad de información contenida en un suceso de probabilidad 1/2)—.

[37] *Vid. v. gr.* https://es.wikipedia.org/wiki/Sistema_ternario.

- según John Florian SOWA [40] (págs. 39–40):

  0. un *vocabulario*, que contiene como vocablos:

     0. *signos lógicos* como los juntores (por ejemplo, ∨ —«o»—) o los cuantores (por ejemplo, ∃ —«existe»—);

     1. *variables*, que representan cualesquiera entidades —objetos, conceptos, propiedades, relaciones— en el universo de aplicación y cuyo rango está definido por los cuantores;

     2. *constantes*, instancias de las variables, esto es, identifican entidades —objetos, conceptos, propiedades, relaciones— particulares en el universo de aplicación;

     3. *signos de puntuación* para agrupar o separar los otros signos;

  1. una *sintaxis* —que estudie las relaciones entre los vocablos independientemente de lo designado y que determine cómo construir fórmulas correctas a partir de fórmulas correctas dadas— y en particular una *teoría de la demostración*;

  2. una *semántica* —esto es, el estudio de las relaciones entre los vocablos y su significado (las entidades y conceptos que designan)— y en particular una *teoría de modelos*; dicha semántica consiste en

     0. una *teoría de referencia* que determine cómo se asocian las constantes y variables a las entidades del universo de discurso y

     1. una *teoría de la verdad* que determine cómo distinguir los enunciados verdaderos de los falsos;

  3. unas *reglas de inferencia*, esto es, unas normas que determinen cómo se infiere una fórmula a partir de otras, lo que nos servirá para caracterizar la *validez* de un argumento —si además el argumento preserva la verdad, decimos que es *sólido*—;

- a lo que debiésemos añadir la *pragmática*[38], esto es, el estudio profundo de las conexiones y relaciones entre los vocablos, su uso y las personas que los usan —interrelaciones entre el cómo, porqué y para qué—[39].

  Todo ello conforma la que pudiésemos llamar una *teoría formal de una lógica*.

[38] *Cfr. v. gr.* REYES [38].
[39] *Cfr. v. gr.* PUTNAM [41].

§ 0.7 El lenguaje $\mathcal{L}_0$ de la lógica de juntores

§ 0.7.0 El vocabulario

La colección de signos componentes de una proposición se denomina *sentencia* y los propios signos, *signos sentenciales*. En particular, los signos sentenciales que representan proposiciones simples de la lógica de juntores se denominan *variables proposicionales*, que se simbolizan por letras latinas minúsculas $p, q, r, s, \ldots, p', q', r', s', \ldots, p'', q'', r'', s'', \ldots, p_0, p_1, p_2, \ldots$; también se las conoce como *variables de enunciado*, *letras sentenciales enunciativas*, *símbolos proposicionales* o *símbolos de enunciado*. Notaremos una variable proposicional genérica por υ.

Definición 0.20.— Formalmente, el lenguaje $\mathcal{L}_0$ —o simplemente $\mathcal{L}$—[40] de la lógica de juntores se define mediante un alfabeto[41] compuesto por:

0. una colección infinita numerable $\mathcal{V}$ de variables proposicionales, es decir, tantas como números naturales,

1. una colección finita $\mathcal{J}$ de símbolos lógicos de enlace entre dichas letras, $\mathcal{J} = \{\bot, \mathrm{id}, \neg, \top\} \cup \{\bot, \mathrm{id}_0, \mathrm{id}_1, \neg_0, \neg_1, \vee, \wedge, \veebar, \barwedge, \rightarrow, \leftarrow, \nrightarrow, \nleftarrow, \leftrightarrow, |, \downarrow, \top\}$, según la notación que estableceremos más adelante, conocidos como *términos de enlace*, *conectores* o *conectivas* y que nosotros llamaremos *juntores*, denominación que se debe a LORENZEN. Observemos que los juntores son un tipo particular de funtores[42]. Dichos juntores pueden ser *monádicos* —también llamados *monoargumentales*, *monarios* o *unitarios*—, caso de que afecten a una única proposición, o *diádicos* —también llamados *biargumentales* o *binarios*—, caso de que enlacen dos proposiciones, existiendo cuatro juntores monádicos y dieciséis juntores diádicos —si bien también insistiremos en que dos de esos juntores pueden considerarse *medádicos*, esto es, no afectan a ninguna proposición, y son la tautología ($\top$) y la contradicción ($\bot$)—, y

2. una colección finita de signos ortográficos[43], de puntuación y auxiliares, con funciones organizativas, de delimitación, determinación o aclaración, entre otras; algunos ejemplos son: () (paréntesis —redondos—), [] (corchetes —paréntesis cuadrados]), {} (llaves —paréntesis aquillados o aballestados—), ⟨⟩ (corchetes angulares), etc.

§ 0.7.1 La fórmula

Definición 0.21.— Decimos de una variable proposicional que es una *fórmula atómica* de $\mathcal{L}_0$.

[40] La razón del subíndice 0 es porque a veces la lógica de juntores se refiere como una lógica de orden cero.
[41] *Vid. supra* § 7 (pág. lxxxv de esta edición).
[42] *Vid. supra* § 0.4.7 (pág. 42 de esta edición).
[43] *Cfr. v. gr.* https://www.rae.es/dpd/signos ortográficos.

Definición 0.22.— Sea $J \subseteq \mathcal{J}$. Una *fórmula* —de $\mathcal{L}_0$— *generada por* J es toda fila de signos que satisfaga alguna de las siguientes condiciones:

F0. las variables proposicionales, p, q, r . . ., son fórmulas;

F1. si $\neg$ es un juntor de J, entonces una fórmula precedida de $\neg$ es una fórmula;

F2. una fórmula, seguida de un juntor de J distinta de $\neg$, seguida de una fórmula, y habiendo hecho buen uso de los paréntesis, es una fórmula.

Pues bien, si $J = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\} \subseteq \mathcal{J}$, entonces llamamos a dicha fórmula generada por J, simplemente *fórmula* (o, sinónimamente, *fórmula bien formada*, *expresión proposicional significativa*, *expresión bien formada*, *forma proposicional*, *forma enunciativa* o *forma lógica*).

La anterior es una definición inductiva. El paso base es el primero y el paso inductivo lo conforman los dos siguientes. Así, partiendo de $J = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$, únicamente son fórmulas las filas de signos obtenidas aplicando alguna de las tres condiciones. En otras palabras, para $J = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$, mediante la definición anterior, obtenemos el conjunto de todas las fórmulas de la lógica de juntores. Notaremos este conjunto por $\mathcal{F}_0$.

Aún más, por suceder precisamente esto decimos que $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ es una base de juntores.

Definición 0.23.— Decimos que un conjunto J de juntores es una *base de juntores* (baj) (o, sinónimamente, *conjunto adecuado de conectores/juntores* [cac], *conjunto completamente expresivo de conectores/-juntores*, *conjunto completo de conectores/juntores* o *conjunto funcionalmente completo de conectores/juntores*) precisamente si mediante la definición 0.22 (pág. 49 de esta edición) obtenemos el conjunto $\mathcal{F}_0$ de todas las fórmulas de la lógica de juntores.

Observación 0.7.0.— En los textos en inglés, en vez de $\mathcal{F}_0$, se usa con frecuencia $\mathcal{W}$, $\mathcal{W}_0$ o $\mathcal{W}_{PL}$ para designar al conjunto de todas las fórmulas; esto proviene del inglés «*well-formed formula (wff)*».

Teorema 0.10
Un conjunto de juntores es una base de juntores si, y sólo si, todos los demás juntores pueden definirse en función únicamente de los del conjunto.

Estudiaremos las bases de juntores en el ámbito semántico en § 1.15 (pág. 161 de esta edición).

Ejemplo 56

Expresemos el silogismo hipotético —*cfr.* ejemplo 52 (pág. 44 de esta edición) en el lenguaje $\mathcal{L}_0$ de la lógica de juntores.

Resolución.— La traducción literal a $\mathcal{L}_0$ del silogismo hipotético es

$$\{\to\}_2(\{\wedge\}_2(\{\to\}_2(x)(y))(\{\to\}_2(y)(z)))(\{\to\}_2(x)(z))),$$

que, relajando un poco la notación, queda

$$\to(\wedge(\to(x)(y))(\to(y)(z)))(\to(x)(z)),$$

o, alternativamente,

$$\to(\wedge(\to(x,y),\to(y,z)),\to(x,z)),$$

en la que se conoce como *notación prefijo* —*cfr. notación polaca*, actividad 1.21 (pág. 174 de esta edición)—; similarmente, en *notación postfijo*,

$$(((x,y)\to,(y,z)\to)\wedge,(x,z)\to)\to,$$

y, definitivamente, en *notación infijo*, con la que seguramente tengamos y tendremos más manejo en estas notas,

$$((x\to y)\wedge(y\to z))\to(x\to z),$$

por ser precisamente la que corresponde a la definición 0.22 (pág. 49 de esta edición) —siendo $J=\{\neg,\wedge,\vee,\to,\leftrightarrow\}$, «una fórmula, seguida de un juntor de J distinto de $\neg$, seguida de una fórmula, y habiendo hecho buen uso de los paréntesis»—. ■

Observación 0.7.1.— Una definición más formal de fórmula precisa de la definición de *conjunto inductivo*[44] y *clausura inductiva*[45], resultando el conjunto $\mathcal{F}_0$ de todas las fórmulas de la lógica de juntores ser la clausura inductiva del conjunto $\mathcal{V}$ de las variables proposicionales, para el conjunto de constructores que corresponden a definir los juntores implicados —por ejemplo, el constructor correspondiente al conjuntor sería $\sigma_\wedge(p,q)=p\wedge q$, siendo p y q dos palabras cualesquiera del alfabeto—. Esta clausura inductiva es, además, una *clausura libremente generada*[46].

Notaremos las fórmulas con letras griegas minúsculas[47] $\phi,\psi,\chi,\tau\ldots$, ocasionalmente con subíndices numéricos, $\phi_0,\phi_1,\phi_2\ldots$; se denominan *variables sintácticas*.

Para notar una *colección de fórmulas* —o una secuencia, vacía o no de ellas— utilizaremos letras griegas mayúsculas $\Gamma,\Delta,\Phi,\Psi\ldots$

[44] *Vid. infra* § 16.4.0 (pág. 817 de esta edición).
[45] *Cid. infra* § 16.4.1 (pág. 818 de esta edición).
[46] *Vid. infra* § 16.4.2 (pág. 819 de esta edición).
[47] El alfabeto griego: α, A (alfa); β, B (beta); γ, Γ (gamma); δ, Δ (delta); ϵ, ε, E (épsilon); ζ, Z (dseta); η, H (eta); θ, Θ (zeta); ι, I (iota); κ, K (kappa); λ, Λ (lambda); μ, M (mi/mu); ν, N (ni/nu); ξ, Ξ (xi); o, O (ómicron); π, ϖ, Π (pi); ρ, ϱ, P (ro); $\sigma, \varsigma, \Sigma$ (sigma), τ, T (tau); υ, Υ (ipsilon); ϕ, φ, Φ (fi); χ, X (ji/chi); ψ, Ψ (psi); ω, Ω (omega).

Ejemplo 57

Aclaremos el hecho de ser fórmula de $\mathcal{L}_0$ o no serlo con algunos ejemplos.

Resolución.— Veamos, dos de fórmula y uno de no fórmula:

- $p \to (q \to p)$ es una fórmula de $\mathcal{L}_0$;
- $\neg p \to (p \to q)$ es una fórmula de $\mathcal{L}_0$;
- la fila de signos $p)q\wedge \to (r\neg \vee q$ no es una fórmula de $\mathcal{L}_0$. ■

Actividad 0.2

¿Es $(p \to q) \veebar (q \to p)$ una fórmula de $\mathcal{L}_0$ generada por la base de juntores $J = \{\veebar, \to\}$?

§ 0.7.2 La subfórmula

Definición 0.24.— Llamamos *subfórmula* de una fórmula ϕ a toda fila de signos consecutivos de ϕ que sea a su vez una fórmula. ϕ^ψ designa el hecho de ser ψ una subfórmula de ϕ. S_ϕ designará el *conjunto de las subfórmulas* de ϕ, esto es, $S_\phi = \{\psi : \phi^\psi\}$.

Ejemplo 58

¿Por qué q no es subfórmula de $p)q\wedge \to (r\neg \vee q$?

Resolución.— Porque aunque q es una fórmula de $\mathcal{L}_0$, $p)q\wedge \to (r\neg \vee q$ no lo es. ■

Definición 0.25.— Sea $J \subseteq \mathcal{J}$ y ϕ una *fórmula* de $\mathcal{L}_0$ generada por J. Una subfórmula de ϕ es toda fila de signos que satisfaga alguna de las siguientes condiciones:

S0. toda variable proposicional, $p, q, r \ldots$ que aparezca en ϕ es subfórmula de ϕ;

S1. si $\neg$ es un juntor de J, entonces una subfórmula de ϕ precedida de $\neg$ es una subfórmula de ϕ;

S2. si una subfórmula de ϕ es de la forma $\chi * \tau$, con $*$ un juntor de J distinto de $\neg$, entonces χ y τ son subfórmulas de ϕ.

Teorema 0.11

$S_{\phi*\psi} = S_\phi \cup S_\psi \cup \{\phi * \psi\}$, para cualesquiera ϕ y ψ fórmulas de $\mathcal{L}_0$.

Ejemplo 59

Si $\phi \coloneqq p \to (q \to p)$, hallemos S_ϕ.

Resolución.—

$$
\begin{aligned}
S_\phi &= S_p \cup S_{q\to p} \cup \{p \to (q \to p)\} && \text{[por el teorema 0.11]}\\
&= S_p \cup S_q \cup S_p \cup \{q \to p\} \cup \{p \to (q \to p)\} && \text{[por el teorema 0.11]}\\
&= \{p\} \cup \{q\} \cup \{p\} \cup \{q \to p\} \cup \{p \to (q \to p)\} && \text{[por la definición 0.24]}\\
&= \{p, q, q \to p, p \to (q \to p\} && \text{[por la definición 10.15].}
\end{aligned}
$$
■

§ 0.7.3 Añadidos a $\mathcal{L}_0$

Hasta ahora, como signos denotativos e identificadores hemos utilizado letras latinas y griegas, con una pluralidad de sentidos:

- con las primeras letras minúsculas latinas $a, b, c, d\ldots$, anotadas o no por subíndices, $a_0, a_1\ldots$, hemos denotado las constantes individuales, que representan entidades concretas;
- con las últimas letras minúsculas latinas x, y, z, anotadas o no por subíndices, $x_0, x_1\ldots$, hemos notado las variables individuales, que representan entidades arbitrarias;
- con las letras mayúsculas latinas $P, Q, R\ldots$, anotadas o no por subíndices, $P_0, P_1\ldots$, hemos notado las letras predicativas, que representan predicados —propiedades, relaciones—;
- con letras latinas mayúsculas $A, B, C\ldots$, anotadas o no por subíndices, $A_0, A_1\ldots$, hemos notado las variables semánticas, que representan proposiciones —simples o compuestas—;
- con letras latinas minúsculas, $p, q, r\ldots$, anotadas o no por subíndices, $p_0, p_1\ldots$, hemos notado las variables proposicionales, que representan proposiciones simples;
- con letras griegas minúsculas, $\phi, \psi, \chi, \tau\ldots$, anotadas o no por subíndices, $\phi_0, \phi_1\ldots$, hemos notado las variables sintácticas, que representan las fórmulas —formas proposicionales—, y
- con letras griegas mayúsculas, $\Gamma, \Delta, \Phi, \Psi\ldots$, anotadas o no por subíndices, $\Phi_0, \Phi_1\ldots$, hemos representado colecciones de fórmulas.

§ 0.7.4 La potencia de un juntor

¿A qué es igual $1 + 2 \cdot 3$?, ¿a 9 o a 7? Casi seguro que el 100 por cien respondemos 7; pero démonos cuenta de que lo hacemos porque *asociamos* en la forma $1 + (2 \cdot 3)$. Más que la fuerza de la costumbre, lo que nos enseñaron, seguro. Y es que existe una regla que nos permite quitar los paréntesis, a saber,

que el producto actúa antes que la suma —siempre que, como aquí, el producto sea una abreviatura de la suma: $2 \cdot 3 = 3 + 3 = 2 + 2 + 2$—.

En general, es cuestión de fijar unos criterios; por ejemplo, si conviniésemos en que los siguientes ocho juntores actúen según el orden $\neg, \wedge, \vee, \veebar, \rightarrow, \leftrightarrow, |, \downarrow$ y, además, en que el orden de actuación de juntores iguales es de izquierda a derecha, tendrían que usarse muchos menos paréntesis. Por ejemplo, la siguiente expresión

$$(p \vee (q \wedge r)) \leftrightarrow ((p \vee q) \wedge ((p \vee r) \downarrow (p \wedge r))),$$

quedaría

$$p \vee q \wedge r \leftrightarrow (p \vee q) \wedge (p \vee r \downarrow p \wedge r).$$

Sin embargo, esto puede provocar una pérdida en la claridad de la expresión y, por otro lado, las convenciones de órdenes de actuación parecerían depender de quienes escribiesen los textos.

En lo que sí parece estar la mayoría de acuerdo es en la siguiente definición.

Definición 0.26.— Decimos que un juntor es *más potente* que otro precisamente si actúa después o, similarmente, un juntor es *más débil* que otro si actúa antes.

Observación 0.7.2.— Esto es similar a decir que en la aritmética elemental el conector $+$ es más potente que $\cdot$ en $1 + 2 \cdot 3$ y, por tanto, no son necesarios los paréntesis $1 + (2 \cdot 3)$. Sin embargo, no ocurre así en la lógica de juntores, donde como veremos justo a continuación, consideramos que los juntores $\vee$ y $\wedge$ tienen igual potencia y sí son necesarios los paréntesis como en $p \vee (q \wedge r)$.

Orden de prelación de juntores

Se acepta el siguiente *orden de prelación de juntores*:

0. que $\neg$ es el juntor de menor potencia;
1. que $\wedge$ es el juntor que sigue en potencia, y ésta es igual a la de $\vee$ y la de $\veebar$;
2. que los demás, salvo $\rightarrow$ y $\leftrightarrow$, son los que siguen según sus potencias, siendo éstas iguales, y
3. que $\rightarrow$ es el juntor de mayor potencia y ésta es igual a la de $\leftrightarrow$.

Reglas de uso de paréntesis

Además, se adoptan las siguientes *reglas de uso de paréntesis*:

0.ª, la negación de una proposición simple no requiere paréntesis, por ejemplo: $\neg(p)$ queda $\neg p$;

1.ª, la negación de una proposición compuesta sí necesita paréntesis, por ejemplo: $\neg(p \wedge q)$ no es $\neg p \wedge q$;

2.ª, varios $\neg$ consecutivos no requieren paréntesis, por ejemplo: $\neg\neg\neg p$ es $\neg(\neg(\neg p))$;

3.ª, la coexistencia de juntores distintos pero de igual potencia sí requiere paréntesis, por ejemplo, sin usar paréntesis, $p \to q \leftrightarrow r$ es ambigua, pues puede interpretarse como $(p \to q) \leftrightarrow r$ o $(p \to (q \leftrightarrow r)$;

4.ª, la coexistencia de conjuntores ($\wedge$) no requiere paréntesis: $p \to q \wedge r \wedge s$ es $p \to (q \wedge r) \wedge s$ y también $p \to q \wedge (r \wedge s)$;

5.ª, la coexistencia de disyuntores ($\vee$) no requiere paréntesis;

6.ª, la coexistencia de contravaledores ($\veebar$) no requiere paréntesis;

7.ª, la coexistencia de equivaledores ($\leftrightarrow$) no requiere paréntesis, y

8.ª, la coexistencia de implicadores ($\to$) sí requiere paréntesis.

Observación 0.7.3.— Si un juntor como operación satisface la propiedad asociativa, no requiere paréntesis.

Observación 0.7.4.— En cualquier caso, ante la duda, usemos paréntesis, que ya lo afirma el refrán: «más vale que sobre que no que falte».

§ 0.7.5 Grado lógico, signo dominante y alcance

Definición 0.27.— Llamamos:

0. *grado lógico* de una fórmula al número de juntores que posee contando las repeticiones (por lo que el grado lógico de una variable proposicional es cero);
1. *signo dominante* de una fórmula (compuesta) al juntor más potente de la misma, y
2. *alcance* de un juntor en una fórmula al conjunto de fórmulas o subfórmulas del cual sea signo dominante.

Ejemplo 60

Sea la fórmula $(p \to q) \wedge \neg p \to q$. Hallemos:

0. su grado lógico;
1. su signo dominante, y
2. el alcance de $\wedge$ en ella.

Resolución.— Hallémoslos:

0. su grado lógico es 4 pues éste es el número de juntores contando las repeticiones (dos $\rightarrow$ más un $\neg$ más un $\wedge$);

1. su signo dominante es $\rightarrow$ (el segundo comenzando por la izquierda);

2. el alcance de $\wedge$ en dicha fórmula es $\{p \rightarrow q, \neg p\}$. ■

§ 0.7.6 Árbol-fórmula

Definición 0.28.— El *árbol-fórmula* de una fórmula es su representación en forma de árbol enraizado ordenado[48]. Dada una fórmula ϕ, decimos que un árbol es el árbol-fórmula de ϕ, y notamos T_ϕ, si satisface:

0. T_ϕ es un árbol enraizado ordenado finito.

1. Los nodos no hojas de T_ϕ son juntores, salvo $\bot$ y $\top$.

2. Los nodos hojas de T_ϕ son variables proposicionales o $\bot$ o $\top$.

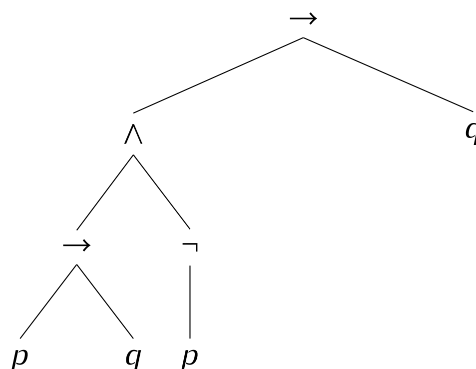
3. Todo nodo no hoja de T_ϕ tiene dos descendientes directos, salvo los nodos correspondientes a $\neg$ y a id que tienen sólo uno.

$T_\top$ es el árbol hoja $\top$ y $T_\bot$ es el árbol hoja $\bot$.

Ejemplo 61

Representemos la fórmula lógica $(p \rightarrow q) \wedge \neg p \rightarrow q$ mediante su árbol-fórmula.

Resolución.— La representación de la fórmula lógica $(p \rightarrow q) \wedge \neg p \rightarrow q$ mediante su árbol-fórmula, construido ascendentemente, con los juntores situados en los nodos raíz de los diferentes subárboles y los argumentos en los nodos hoja es



[48] Para la definición de árbol enraizado ordenado, *vid. supra* pág. 183 de esta edición.

Observamos que, como estudiamos en el ejemplo 60 (pág. 55 de esta edición), su grado lógico es cuatro (los cuatro juntores que hay en el árbol), su signo dominante es el segundo implicador (está en la raíz) y el alcance de $\wedge$ es $\{p \to q, \neg p\}$ (las subfórmulas en el subárbol de raíz $\wedge$). ■

Teorema 0.12
Si ψ es una subfórmula de ϕ, entonces T_ψ es un subárbol de T_ϕ.

§ 0.7.7 Literal, cubo y cláusula

Definición 0.29.— Según los juntores que dominen se destacan *algunos tipos de fórmulas*:

0. un *literal* es una variable proposicional o negación de una variable proposicional; los literales p (*literal positivo*) y $\neg p$ (*literal negativo*) se denominan *literales opuestos*; habitualmente λ designa un literal positivo, sea sin o con subíndices: $\lambda_0, \lambda_1 \ldots$;
1. una *fórmula conjuntiva*, también llamada *de tipo* α, es una conjunción de literales;
2. un *cubo* —también llamado *término producto* en el ámbito de los sistemas digitales— es un literal o una fórmula conjuntiva;
3. una *fórmula disyuntiva*, también llamada *de tipo* β, es una disyunción de literales;
4. una *cláusula* —también llamado *término suma* en el ámbito de los sistemas digitales— es un literal o una fórmula disyuntiva.

§ 0.8 Lenguaje y metalenguaje

Cuando afirmamos algo sobre las fórmulas o acerca de interrelaciones entre ellas no estamos empleando el lenguaje $\mathcal{L}_0$ sino otro lenguaje que llamamos *metalenguaje*. En este caso, $\mathcal{L}_0$ es un ejemplo de *lenguaje objeto* —que también diremos lenguaje situado en un grado/nivel cero de metalenguaje—. Por ejemplo, la fila de signos «$\neg p \vee q$» es una fórmula escrita en el lenguaje $\mathcal{L}_0$; sin embargo, toda la afirmación, esto es, «la fila de signos “$\neg p \vee q$” es una fórmula escrita en el lenguaje $\mathcal{L}_0$» está escrita en el metalenguaje.

Convenimos en que los nombres de las letras sentenciales y de los juntores en el metalenguaje son ellos mismos, lo que, por ejemplo, nos permite escribir:

- Cuando escribimos $p \vee q$ queremos decir ‘sucede p o sucede q’.
- La fila de signos $p)\neg q$ carece de significado en la lógica de juntores.
- Los signos $\neg$ y $\vee$ son juntores y la sentencia $\neg p$ es una proposición compuesta.

en vez de tener que escribir, respectivamente:

- Cuando escribimos «$p \lor q$» queremos decir 'sucede p o sucede q'.
- La fila de signos «$p)\neg q$» carece de significado en la lógica de juntores.
- Los signos «$\neg$» y «$\lor$» son juntores y la sentencia «$\neg p$» es una proposición compuesta.

Por otro lado, en algunos textos se utiliza la tipografía en *itálica* para el lenguaje objeto y la normal para el metalenguaje —así, $(p \to q) \land p \to q$ es del lenguaje objeto y $(\mathrm{p} \to \mathrm{q}) \land \mathrm{p} \to \mathrm{q}$ es del metalenguaje—, mientras que en otros, se usan letras latinas para el lenguaje objeto y letras griegas para el metalenguaje —así, $(p \to q) \land p \to q$ es del lenguaje objeto y $(\pi \to \theta) \land \pi \to \theta$ es del metalenguaje—.

En estas notas designamos las fórmulas con letras minúsculas del alfabeto griego. Así,

$$\phi \to \psi,$$

que expresa una relación entre dos fórmulas, pertenece en realidad al metalenguaje, y no es una fórmula, pues éstas pertenecen al lenguaje objeto; diremos que es un *esquema de fórmula*, una colección de infinitas fórmulas, una de las cuales podría ser, por ejemplo, la *ley de Clavio* —conocida también como *consequentia mirabilis*—,

$$(\neg p \to p) \to p,$$

si bien, pudiésemos enunciar la propia ley de Clavio en el metalenguaje,

$$(\neg \phi \to \phi) \to \phi,$$

siendo entonces un ejemplo de *instancia* de ella,

$$(\neg(p \lor (q \to r)) \to (p \lor (q \to r))) \to (p \lor (q \to r)).$$

Ejemplo 62

Para los siguientes esquemas de fórmulas —enunciados en el metalenguaje, que son leyes clásicas de la lógica de primer orden—, proporcionemos ejemplos de instancias suyas.

0. $(\neg \phi \to \phi) \to \phi$ (*Consequentia mirabilis*)
1. $(\phi \land \neg \phi) \to \psi$ (*Ex falso quodlibet*)
2. $\neg(\phi \land \neg \phi)$ (*Principium contradictionis*)
3. $(\phi \lor \neg \phi)$ (*Tertium non datur*)

Resolución.— A modo de ejemplo de instancias suyas, las siguientes:

0. $(\neg(p \land q) \to (p \land q)) \to (p \land q)$;

1. $((p \vee q) \wedge \neg(p \vee q)) \rightarrow (p \rightarrow q)$;

2. $\neg((p \vee (\neg r \rightarrow q)) \wedge \neg(p \vee (\neg r \rightarrow q)))$;

3. $((p \leftrightarrow q) \vee \neg(p \leftrightarrow q))$. ■

§ 0.9 A vueltas con el razonamiento: la contraargumentación

Un argumento, sea $\mathcal{A}$, no es más que una interpretación, es decir, una expresión en lenguaje ordinario, en nuestro caso español, de una forma lógica, digamos A, que hemos determinado adecuada para representar a $\mathcal{A}$. Entonces, un `contraargumento` de $\mathcal{A}$ es un argumento en la misma forma lógica que $\mathcal{A}$, esto es, una nueva interpretación de la forma lógica A, tal que la colección de las premisas no justifica su conclusión; su correspondiente `contraargumentación` es un encadenamiento pertinente de oraciones declarativas.

Ejemplo 63

Sea la argumentación: «Si sucede alguna de dos cosas, suceden ambas». Hallemos un argumento que le corresponda, una formalización en lógica de juntores (variables proposicionales, esquema argumental y forma lógica), un contraargumento y una contraargumentación.

[Cubit 8].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si sucede una primera cosa o sucede una segunda cosa, entonces sucede tal primera cosa y sucede dicha segunda cosa.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

   - *Variables proposicionales*:

     Siendo el universo de discurso el conjunto de todas las cosas, las variables proposicionales son:

     $A \leftrightharpoons$ Sucede la cosa A;

     $B \leftrightharpoons$ Sucede la cosa B.

   - *Esquema argumental*:

$$\begin{array}{ll} & \text{Se tiene } A \text{ o } B. \\ \hline \therefore & \text{Se sigue } A \text{ y } B. \end{array}$$

   - *Forma lógica*.

Identificamos el conjunto de premisas $\Phi = \{\phi_0\} = \{A \vee B\}$ y la conclusión ψ, a saber, $A \wedge B$.

La fórmula en lógica de juntores que hemos hallado para $\mathcal{A}$ es

$$A \vee B \rightarrow A \wedge B.$$

A modo de ejemplos de contraargumento y contraargumentación, los siguientes.

2. *Contraargumento*: Si sucede la primera cosa y no sucede la segunda, entonces sucede la primera cosa o sucede la segunda, pero no es cierto que sucedan la primera cosa y la segunda.

3. *Contraargumentación*: Si sucede una de dos cosas no es cierto que sucedan ambas, pues puede que una no suceda. ■

En el ejemplo, el hallazgo de la forma lógica ha sido clave. Esta forma lógica es un esquema de fórmula —de fórmulas en relación— perteneciente al metalenguaje. Así vemos cómo el metalenguaje ayuda, sin duda, a encontrar contraargumentaciones.

Si hacemos partícipe a la semántica pudiésemos comprobarlo, por ejemplo, mediante una tabla de verdad[49].

§ 0.10 Bibliografía

- Debo mucho al conocimiento y manera de exponerlo de Joaquín Carreras Artau y de Antonio Aróstegui Megías, respectivamente, en:

[42] Joaquín Carreras Artau. *Introducción a la filosofía (lógica, psicología y ética)*. Alma Mater, Barcelona, Cataluña (ES-CT), España, 4.ª ed., 1944.

[43] Antonio Aróstegui Megías. *Curso de concienciación filosófica*. Marsiega, Madrid, Comunidad de Madrid (ES-M), España, 1977.

- Para expandir horizontes, creo adecuado, entre muchos, el libro de John Florian Sowa:

[40] John Florian Sowa. *Knowledge Representation. Logical, Philosophical, and Computational Foundations*. Brooks/Cole, Pacific Grove, California, 2000.

[49] *Vid. infra* definición 1.2 (pág. 65 de esta edición).

Capítulo **1**

De la semántica. I

Dados dos blips distintos cualesquiera, existe exactamente una nipa que los contiene.
(Philip J. Davis y Reuben Hersh).

¿Qué sería del mundo sin el significado de las cosas?

§ 1.0 La interpretación, el modelo y el contramodelo

La semántica, saber de las significaciones de los signos y sus combinaciones, también ayuda a encontrar contraargumentaciones.

En los artículos anteriores han aparecido proposiciones compuestas y esquemas de fórmulas en relación, por ejemplo, la forma lógica $\phi \vee \psi \rightarrow \phi \wedge \psi$ en el ejemplo 63 (pág. 59 de esta edición). Aunque pudiésemos profundizar en el estudio de la coordinación entre proposiciones desde la sintaxis, como un juego de letras, prefiero que lo hagamos haciendo partícipe la semántica y la pragmática, ¡no en vano somos criaturas humanas!

Nuestro interés, en definitiva, radica en la decodificación de los signos de expresiones sintácticas con el fin de determinar los mensajes de dichas expresiones (su contenido semántico) y, recíprocamente, en la codificación de un significado en una combinación de signos sintácticos.

Como afirma Esther Torrego [44] (pág. 139), el aprendizaje de una lengua no materna (L1) —lenguaje lógico-matemático, en nuestro caso— se diferencia de la adquisición de una lengua materna (L0): 0.º, la adquisición de una segunda lengua requiere esfuerzo consciente; 1.º, no se obtienen resultados uniformes con su aprendizaje; 2.º, la lengua segunda interfiere frecuentemente con la lengua materna y con otras lenguas segundas aprendidas, y 3.º, los procesos de imitación y memorización son esenciales.

Esto hace que debamos prestar máxima atención a los procesos de *traducción directa* —de L1 a L0— y *traducción inversa* —de L0 a L1—; tarea que nos llevará unas páginas.

§ 1.0.0 La interpretación

Pensemos en la expresión verbal «Toda criatura humana comete errores»°. Si tuviésemos que decir si es verdadera o falsa, seguramente diríamos que es verdadera, por lo que estaríamos ante una proposición. Entonces, pudiésemos también decir que su *valor de verdad* es verdadero, que denotaremos por 1 (o, sinónimamente, V), en oposición a falso, que denotaremos por 0 (o, sinónimamente, F).

Notemos que si hubiésemos elegido el camino de la sintaxis en soledad, estas mismas cuatro grafías 0, 1 (o F y V) serían sólo dos letras que se combinarían conforme a las reglas del juego sintáctico, aunque el significado no se asomaría por ningún lado.

° Decía Alan Turing que cometer errores es parte esencial de la inteligencia observada y, por ende, de cualquier inteligencia artificial. Mas esto no deja de ser compararla con la humana. Pensemos en un pájaro y en un avión. No sé si ambos vuelan, pero, sin duda, ambos utilizan el aire como medio para trasladarse de un lugar a otro, y esto, a pesar de que las formas en que lo hacen no se asemejan.

Si A representa una proposición, la expresión simbólica

$$[\![A]\!]$$

significa 'el valor de verdad de la proposición designada por A'. También se usan las designaciones $|A|$ e $I(A)$ (la 'I' es de interpretación[1]).

Así, si

$$A \leftrightharpoons \text{«Toda criatura humana comete errores»},$$

pudiésemos escribir $[\![A]\!] = 1$, $|A| = 1$ o $I(A) = 1$.

De aquí en adelante utilizaremos las denotaciones 0 y 1.

Definición 1.0.— Decimos que el *valor de verdad* —concepto acuñado sobre 1879 por Frege y Peirce— de una fórmula ϕ es 1 cuando es verdadera, y 0 cuando es falsa.

De aquí el nombre de *lógica bivalente*.

Observación 1.0.0.— Existen muchos tipos de lógicas, entre ellas, por ejemplo, las *lógicas polivalentes*[2], en la cual, una proposición puede tener un cierto grado de verdad o falsedad; por ejemplo, «mañana lloverá», de ser imposible hoy tener la certeza de su verdad o falsedad, en lógica bivalente no sería una proposición hasta el día siguiente, que comprobásemos si llueve o no. Pero en lógica polivalente asignamos al hecho de ser falso el valor 0, al hecho de ser cierto el valor 1 y si, por ejemplo, esperamos que llueva con un 70 por ciento de posibilidades, decimos que el *grado de verdad* de la anterior proposición es 0,7.

Definición 1.1.— Llamamos *interpretación* a cualquier función $I : \mathcal{V} \to \{0, 1\}$. Una *interpretación para una fórmula* ϕ es la restricción de una interpretación al subconjunto $V_\phi(\subset \mathcal{V})$ de variables de enunciado que aparecen en ϕ, esto es, una asignación de valores de verdad a todas y cada una de dichas variables de enunciado. Esta asignación determinará, como veremos más adelante, el valor de verdad de la fórmula.

De este modo, el valor de verdad de una variable proposicional p no es más que la imagen por alguna interpretación. Por ello, también lo notaremos por $I(p)$. Cuando ϕ sea una fórmula compuesta, $I(\phi)$ designará su valor de verdad[3].

Siendo ϕ una fórmula y w una secuencia finita de valores de verdad, emplearemos la notación $I_w(\phi)$ o $I(\phi, w)$ para mayor especificidad; por ejemplo, si ϕ es una fórmula tal que sus variables de enunciado son p, q y r, notaremos $I_{010}(\phi)$ o $I(\phi, 010)$, donde 010 abrevia la asignación simultánea

1 *Vid. infra* definición 1.1 (pág. 64 de esta edición).
2 *Vid. infra* § 9.1 (pág. 519 de esta edición).
3 *Cfr. infra* definición 1.17 (pág. 123 de esta edición).

$\langle p, q, r \rangle \leftarrow\!\!\dashv \langle 0, 1, 0 \rangle$, esto es, la interpretación $I(p) = 0$, $I(q) = 1$, $I(r) = 0$, o abreviadamente, $I\langle p, q, r \rangle = \langle 0, 1, 0 \rangle$.

§ 1.0.1 La tabla de verdad

Definición 1.2.— Una *tabla de verdad* para una fórmula es una disposición rectangular de los valores de verdad de la misma, teniendo tantas filas como interpretaciones y figurando en cada fila una, y sólo una, de sus interpretaciones.

Ejemplo 64

¿Cuál es la tabla de verdad de ϕ si sus únicas variables de enunciado son p y q?

Resolución.— Si las únicas variables de enunciado de ϕ son p y q, entonces la tabla de verdad de ϕ es

p	q	ϕ
1	1	$I_{11}(\phi)$
1	0	$I_{10}(\phi)$
0	1	$I_{01}(\phi)$
0	0	$I_{00}(\phi)$

que también es posible notar

p	q	ϕ
1	1	$[\![\phi]\!]_{11}$
1	0	$[\![\phi]\!]_{10}$
0	1	$[\![\phi]\!]_{01}$
0	0	$[\![\phi]\!]_{00}$

Usaremos cualquiera de estas notaciones indistintamente. ■

Observación 1.0.1.— La tabla tiene tantas filas como interpretaciones conjuntas de todas las variables de la fórmula —p y q, en este caso—; dichas interpretaciones no son más que los valores $I\langle p, q \rangle$, esto es, $\langle 1, 1 \rangle$, $\langle 1, 0 \rangle$, $\langle 0, 1 \rangle$ y $\langle 0, 0 \rangle$. Por ello, asimismo, los valores $1, 1, 0, 0$ en la columna «p» corresponden a interpretaciones de p, esto es, son valores $I(p)$ y los $1, 0, 1, 0$ de la columna «q» son valores $I(q)$.

Ejemplo 65

Suponiendo verdadera la afirmación «si el programa funciona o habrá más recursos, entonces habrá más recursos», ¿qué podemos concluir si no habrá más recursos?

a. Que el programa funciona.
b. Que el programa no funciona.
c. Que si el programa funciona, habrá más recursos.
d. No podemos concluir nada.

[TT], [EFE 3.7.2024:0] (tipo test), [EFE 29.1.2025:0] (tipo test) (c. Que si el sistema está operativo, se incrementará la capacidad), [EFEC 29.1.2025:0] (tipo test) (c. Que si la aplicación está activa, se aumentará la memoria).

Resolución.—

0. Llamemos $\mathcal{A}$ al argumento dado.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales*:

     Siendo el universo de discurso el conjunto de todos los programas, consideramos dos variables proposicionales y las proposiciones simples que representan:

     $p \risingdotseq$ El programa funciona;

     $q \risingdotseq$ Habrá más recursos.

   - *Esquema argumental*:

     Si se supone que,
     bien que el programa funciona,
     bien que habrá más recursos,
     bien ambas.

     ∴ Se sigue que habrá más recursos.

   - *Forma lógica.*

     Identificamos el conjunto de premisas $\Phi = \{\phi_0\} = \{p \vee r\}$, con una única premisa, y la conclusión ψ, a saber, r.

     La fórmula en lógica de juntores que hemos hallado para $\mathcal{A}$ es

     $$p \vee r \to r.$$

   - *Resolución del argumento.*

A la vista de la tabla de verdad de $p \lor r \to r$,

p	r	$p \lor r \to r$
1	1	1
1	0	0
0	1	1
0	0	1

tenemos que como por hipótesis $p \lor r \to r$ es verdadera y r falsa, la única interpretación posible es $I^{\langle p,r\rangle}_{\langle 0,0\rangle}$, en particular que p es falsa, en otras palabras, que el programa no funciona.

Solución.— Opción b. ■

Ejemplo 66

Sólo una de las siguientes afirmaciones es verdad.

a. Si $q \to r$ es verdadera, entonces $(p \lor q) \to (p \lor r)$ es falsa.

b. Si $q \to r$ es verdadera, entonces $(p \lor q) \to (p \lor r)$ puede ser verdadera o falsa.

c. Si $q \to r$ es falsa, entonces $(p \lor q) \to (p \lor r)$ puede ser verdadera o falsa.

d. Si $q \to r$ es falsa, entonces $(p \lor q) \to (p \lor r)$ es verdadera.

[TT], [EFE 3.7.2024:3] (tipo test).

Resolución.— A la vista de las tablas de verdad de $q \to r$ y $(p \lor q) \to (p \lor r)$,

p	q	r	$q \to r$	$(p \lor q) \to (p \lor r)$
1	1	1	1	1
1	1	0	0	1
1	0	1	1	1
1	0	0	1	1
0	1	1	1	1
0	1	0	0	0
0	0	1	1	1
0	0	0	1	1

tenemos: si $q \to r$ es verdadera, $(p \lor q) \to (p \lor r)$ es verdadera, por lo que descartamos las opciones a) y b); si $q \to r$ es falsa, $(p \lor q) \to (p \lor r)$ puede ser verdadera —interpretación $I^{\langle p,q,r\rangle}_{\langle 1,1,0\rangle}$— o falsa —interpretación $I^{\langle p,q,r\rangle}_{\langle 0,1,0\rangle}$—, por lo que la opción verdadera es la c).

Solución.— Opción c. ■

Actividad 1.0

Sólo una de las siguientes afirmaciones es verdad.

a. Si $p \to q$ es verdadera, entonces $(\neg p \wedge q)$ es verdadera.
b. Si $p \to q$ es verdadera, entonces $(\neg p \wedge q)$ es falsa.
c. Si $p \to q$ es falsa, entonces $(\neg p \wedge q)$ puede ser verdadera o falsa.
d. Si $p \to q$ es falsa, entonces $(\neg p \wedge q)$ es falsa.

[Cubit 10], [TT], [EFE 29.1.2025:3] (tipo test), [EFEC 29.1.2025:3] (tipo test).

Con miras a su resolución.— Procedamos de manera similar a lo hecho en el ejemplo 66 (pág. 67 de esta edición). Observando las tablas de verdad de $p \to q$ y de $\neg p \wedge q$ —utilicemos, por ejemplo, el artefacto en línea Wolfram|Alpha[4] con la petición `p implies q, not p and q`—, observamos que: si $p \to q$ es verdadera, $\neg p \wedge q$ puede ser verdadera (I_{01}) o falsa (I_{11} e I_{00}) y que si $p \to q$ es falsa, $\neg p \wedge q$ es necesariamente falsa (I_{10}); en definitiva, la opción verdadera es la d.

Actividad 1.1

Suponiendo verdadera la afirmación «una palabra no es palíndroma siempre que sea polisémica o sobreesdrújula», ¿qué podemos concluir sobre la palabra RECONOCER, que claramente es palíndroma?

a. Que o no es polisémica o no es sobreesdrújula.
b. Que es polisémica y sobreesdrújula.
c. Que es falso que sea polisémica y sobreesdrújula.
d. Que no es ni polisémica ni sobreesdrújula.

[Cubit 11], [TT].

Con miras a su resolución.— La forma lógica de la afirmación es $t \vee s \to p$, donde las variables proposicionales son: $t \leftrightharpoons$ La palabra es polisémica; $s \leftrightharpoons$ La palabra es sobreesdrújula; $p \leftrightharpoons$ La palabra es palíndroma. En la tabla de verdad de dicha forma lógica —utilicemos, por ejemplo, el artefacto en línea Wolfram|Alpha[5] con la petición `tabla de verdad (t or s) implies not p`—, observamos que la única interpretación verdadera (debe ser verdadera porque suponemos verdadera la afirmación) en la que p es verdadera (debe ser verdadera porque RECONOCER es palíndroma) es $I^{\langle t,s,p\rangle}_{\langle 0,0,1\rangle}$, lo cual significa que RECONOCER no es ni polisémica ni sobreesdrújula; en definitiva, la única verdadera es la opción d.

Actividad 1.2

Escuchamos a Jerónimo Román (JR) hablar en voz alta sobre lo que hizo ayer tarde: «Inicialicé la variable x, ¿o fue la y?, ¿o las dos?» [...] «Lo que sí tengo claro es que si hubiese inicializado la variable z, habría actualizado la variable s.» [...] «Pero no actualicé las variables s y t».

---

[4] *Cfr.* https://www.wolframalpha.com/.
[5] *Cfr.* https://www.wolframalpha.com/.

Sabemos que JR es el mayor mentiroso del mundo incluso cuando habla solo, de hecho todo lo que dice es falso, siempre. ¿Qué hizo JR?

a. Inicializó x o inicializó y, y actualizó s y actualizó t.
b. No inicializó ni x ni y; inicializó z; no actualizó s, y no puede asegurarse nada sobre t.
c. No inicializó ni x ni y; inicializó z; no actualizó s, pero sí actualizó t.
d. No inicializó ni x ni y ni z, y no actualizó ni s ni t.

[Cubit 12], [TT].

Con miras a su resolución.— La forma lógica de lo dicho por JR es $\neg(x \vee y) \wedge \neg(z \to s) \wedge \neg(\neg s \wedge \neg t)$, donde las variables proposicionales son: $x \leftrightharpoons$ Inicializa la variable x; $y \leftrightharpoons$ Inicializa la variable y; $z \leftrightharpoons$ Inicializa la variable z; $s \leftrightharpoons$ Actualiza la variable s; $t \leftrightharpoons$ Actualiza la variable t. En la tabla de verdad de dicha forma lógica —utilicemos, por ejemplo, el artefacto en línea Wolfram|Alpha[6] con la petición `tabla de verdad not(x or y) and not(z implies s) and not (not s and not t)`—, observamos que la única interpretación verdadera para ella es $I^{\langle x,y,z,s,t\rangle}_{\langle 0,0,1,0,1\rangle}$, lo cual significa que JR no inicializó ni x ni y, inicializó z, no actualizó s, pero sí actualizó t; en definitiva, la verdadera es la opción c.

§ 1.0.2 El modelo

Llegado este punto nos permitimos identificar la interpretación I_w con la variación con repetición w; así hablaremos de la interpretación 101 o I_{101}, indistintamente.

Definición 1.3.— Decimos que la interpretación w es un *modelo para la fórmula* ϕ precisamente si ϕ es verdadera con la interpretación w, es decir, precisamente si $I_w(\phi) = 1$; $\mathcal{M}(\phi)$ designa el conjunto de todos los modelos para la fórmula ϕ, esto es, $\mathcal{M}(\phi) = \{w : I_w(\phi) = 1\}$.

Definición 1.4.— Decimos que la interpretación w es un *modelo para el conjunto de fórmulas* Φ precisamente si w es un modelo para toda fórmula de Φ; $\mathcal{M}(\Phi)$ designa el conjunto de todos los modelos para el conjunto de fórmulas Φ.

Teorema 1.0

$\mathcal{M}(\Phi) = \bigcap_{\phi \in \Phi} \mathcal{M}(\phi)$.

Ejemplo 67

Demostremos que no existe ningún modelo para el conjunto de fórmulas $\{p, \neg p\}$.

[6] *Cfr.* https://www.wolframalpha.com/.

Resolución.— Esto es así porque las únicas interpretaciones de p son I_1 e I_0 por lo que sólo son dos las valoraciones de verdad de las fórmulas de $\{p, \neg p\}$, a saber,

p	p	$\neg$	p
1	$\boxed{1}$	$\boxed{0}$	1
0	$\boxed{0}$	$\boxed{1}$	0

y, como observamos, los únicos pares de valores de verdad posibles son $\langle 1, 0\rangle$ y $\langle 0, 1\rangle$. ■

Ejemplo 68

Demostremos que la interpretación $I(p) = 0$, $I(q) = 0$ es un modelo para el conjunto de fórmulas $\Phi = \{p \leftrightarrow q, \neg(\neg p \wedge q)\}$.

Resolución.— En efecto, la valoración de verdad de las fórmulas de Φ con la interpretación I_{00} es

p	q	p	$\leftrightarrow$	q	$\neg$	(	$\neg$	p	$\wedge$	q	)
0	0	0	$\boxed{1}$	0	$\boxed{1}$		1	0	0	0	

en otras palabras, I_{00} es un modelo para $p \leftrightarrow q$ y para $\neg(\neg p \wedge q)$ y, por lo tanto, un modelo para Φ. ■

Observación 1.0.2.— Aunque la hemos ejemplificado en la tabla de verdad del ejemplo 64 (pág. 65 de esta edición), como seguramente leeremos textos que la usen, las designaciones $I(\phi)$, $I_w(\phi)$, se escriben con la otra notación, $[\![\phi]\!]_I$, $[\![\phi]\!]_w$, respectivamente.

Definición 1.5.— Decimos que una tabla de verdad de una fórmula es *tautológica* si todas las interpretaciones son modelos, *satisfactible* si al menos una interpretación es modelo e *insatisfactible* si ninguna interpretación es modelo.

Actividad 1.3

¿Es absurdo afirmar $(p \vee q) \wedge p \rightarrow (p \wedge q) \vee p$?

Con miras a su resolución.— No es absurdo, al contrario, la tabla de verdad de $(p \vee q) \wedge p \rightarrow (p \wedge q) \vee p$ es tautológica.

Actividad 1.4

¿Pudiese ser apropiado afirmar que $((p \vee q) \rightarrow r) \wedge \neg q \rightarrow p \vee r$ es una fórmula *casi válida*?

Con miras a su resolución.— Quizás sí, porque igualmente pudiésemos decir que su tabla de verdad es *casi satisfactible* ya que de sus ocho interpretaciones, siete son modelos (pudiésemos comprobarlo haciendo su tabla de verdad).

§ 1.0.3 El contramodelo

Definición 1.6.— Decimos que la interpretación w es un *contramodelo para la fórmula* ϕ precisamente si ϕ es falsa con la interpretación w, es decir, precisamente si $I_w(\phi) = 0$; $\mathcal{C}(\phi)$ designa el conjunto de todos los contramodelos para la fórmula ϕ, esto es, $\mathcal{C}(\phi) = \{w : I_w(\phi) = 0\}$.

Definición 1.7.— Decimos que la interpretación w es un *contramodelo para el conjunto de fórmulas* Φ precisamente si w es un contramodelo para alguna fórmula de Φ; $\mathcal{C}(\Phi)$ designa el conjunto de todos los contramodelos para el conjunto de fórmulas Φ.

Teorema 1.1

$\mathcal{C}(\Phi) = \bigcup_{\phi \in \Phi} \mathcal{C}(\phi)$.

Definición 1.8.— Sea ϕ la fórmula $\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \rightarrow \psi$. Llamamos *conjunto decisor para* ϕ a cualquier conjunto Γ de fórmulas tal que se satisface que w es un modelo para Γ si, y sólo si, w es un contramodelo para ϕ. Si hay lugar a confusión, pudiésemos designarlo haciendo referencia a ϕ, así: Γ_ϕ.

Teorema 1.2

Sea $\Phi = \{\phi_0, \phi_1, \ldots, \phi_n\}$. Sea $\Gamma = \Phi \cup \{\neg\psi\}$. Sea ϕ la fórmula $\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \rightarrow \psi$. Se satisface que w es un modelo para Γ si, y sólo si, w es un contramodelo para ϕ. En otras palabras, Γ es un conjunto decisor para ϕ.

Observación 1.0.3.— Esta equiparación se registra en lógica de juntores en el hecho de que la tabla de verdad de la fórmula $\neg(\phi \rightarrow \psi) \leftrightarrow \phi \wedge \neg\psi$ es tautológica[7], lo que se corresponde con la equivalencia lógica *principio de* Crisipo[8], con la regla deductiva *negación del implicador* (NI)[9] y con la regla semántica *falsedad de la implicación* (FI)[10].

[7] Más adelante diremos: en la sintaxis, que es un teorema lógico (*cfr. infra* § 2.0 [pág. 177 de esta edición]), y en la semántica, que es una fórmula válida (*cfr. infra* definición 1.11 [pág. 119 de esta edición]).

[8] *Vid. infra* § 1.27 (pág. 166 de esta edición).

[9] *Vid. infra* § 2.2.39 (pág. 218 de esta edición).

[10] *Vid. infra* § 3.3.0 (págs. 275ss. de esta edición) y § 366 (págs. 381ss. de esta edición).

Ejemplo 69

Sean Φ el conjunto $\{p \leftrightarrow q\}$ y ψ la fórmula $\neg p \wedge q$. Hallemos un contramodelo para $(p \leftrightarrow q) \rightarrow (\neg p \wedge q)$.

Resolución.— En el ejemplo anterior hemos demostrado que la interpretación I_{00} es un modelo para $\Phi \cup \{\neg\psi\}$, esto es, para Γ. Pues bien, dicha interpretación, I_{00}, es un contramodelo para $(p \leftrightarrow q) \rightarrow (\neg p \wedge q)$, como apreciamos en la tabla de verdad

p	q	(	p	$\leftrightarrow$	q	)	$\rightarrow$	(	$\neg$	p	$\wedge$	q	)
0	0		0	1	0		$\boxed{0}$		1	0	0	0	

■

Actividad 1.5

¿Pudiésemos afirmar que la fórmula $((p \vee q) \rightarrow r) \wedge \neg r \rightarrow p \wedge q$ es *muy raramente inválida*?

Con miras a su resolución.— Quizás sí, porque igualmente pudiésemos decir que su tabla de verdad es *muy raramente insatisfactible* ya que de sus ocho interpretaciones, sólo una es un contramodelo, a saber, precisamente cuando p, q y r son falsas (pudiésemos comprobarlo haciendo su tabla de verdad).

Ejemplo 70

Hallemos una contraargumentación para la argumentación «Teniendo que suceder una segunda cosa cuando sucede una primera y ésta cuando sucede la segunda, se deduce que, a la vez ocurre que no sucede la primera y sí sucede la segunda».

Resolución.—

0. *Argumento* ($\mathcal{A}$): Llamemos p a la primera cosa y q a la segunda. Si sucede p, entonces sucede q, y si sucede q, entonces sucede p. Luego, no sucede p y, a la vez, sucede q.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales*:

     Considerando como universo de discurso el conjunto de todos los sucesos, sean las siguientes dos variables proposicionales y sus correspondientes significados:

$$p \risingdotseq \text{sucede } p,$$
$$q \risingdotseq \text{sucede } q.$$

- *Esquema argumental*:

$$\begin{array}{rl} & \text{Si se supone } p\text{, se sigue } q\text{, y si se supone } q\text{, se sigue } p. \\ \hline \therefore & \text{Se sigue no } p \text{ y } q. \end{array}$$

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0\} = \{p \leftrightarrow q\}$ y la conclusión ψ, a saber, $\neg p \wedge q$.

  La fórmula en lógica de juntores que hemos hallado para $\mathcal{A}$ es

$$(p \leftrightarrow q) \rightarrow (\neg p \wedge q).$$

  Llamémosla A.

2. *Resolución de $\mathcal{A}$*.

   Por el ejemplo anterior sabemos que la interpretación I_{00} es un contramodelo para A, a saber, caso de que no sucedan ni p ni q, se satisface la premisa pero no así la conclusión. Esto demuestra que $\mathcal{A}$ es un argumento no válido.

   Dicho contramodelo permite construir una contraargumentación y deducir, por lo tanto, que la argumentación no es válida. Para ello, tengamos en cuenta que el hecho de no satisfacerse $\phi_0 \rightarrow \psi$ equivale a que se satisfaga $\phi_0 \wedge \neg\psi$.

A modo de ejemplos de contraargumento y contraargumentación, los siguientes.

3. *Contrargumento*: Si no suceden ni p ni q se satisface lo afirmado por la premisa «si sucede p, entonces sucede q, y si sucede q, entonces sucede p» (ya que no afirma nada caso de que no sucediesen), pero no se satisface lo afirmado por la conclusión «no sucede p y, simultáneamente, sucede q» (ya que no sucede q).

4. *Contraargumentación*: Si no suceden ninguna de dos cosas, una primera y una segunda, es cierta la premisa, pues se mantiene la equivalencia en el suceder ambas a la vez, pero no es cierta la conclusión, a saber, que no suceda la primera y sí la segunda, simple y llanamente, porque no sucede la segunda. ■

§ 1.1 Número de juntores

Teorema 1.3 (Número total de juntores)
En lógica bivalente existe un total de 2^{2^n} funciones veritativas enádicas; esto es, $2^{2^0} = 2$ medádicas (de orden 0), $2^{2^1} = 4$ monádicas (de orden 1), $2^{2^2} = 16$ diádicas (de orden 2), $2^{2^3} = 256$ triádicas (de orden 3), $2^{2^4} = 65\,536$ tetrádicas (de orden 4), etc.

Demostración.— La tabla de verdad de una fórmula en la que aparecen dos variables proposicionales, p y q, tiene cuatro filas, correspondientes a $\langle 1,1\rangle$, $\langle 1,0\rangle$, $\langle 0,1\rangle$ y $\langle 0,0\rangle$, las posibles valoraciones de verdad de $\langle I(p), I(q)\rangle$. Este número de filas es el *número de variaciones con repetición*[11] de dos elementos del conjunto $\{0,1\}$, esto es, $VR(2,2) = 2^2$. El número total de juntores diádicos es el de posibles tablas de verdad de 2^2 filas, esto es, el de variaciones con repetición de 2^2 elementos de $\{0,1\}$ (es decir, éstos tomados de 2^2 en 2^2), que es[11] $VR(2,2^2) = 2^{2^2}$. En general, el número de filas de la tabla de verdad de cualquier fórmula en la que intervienen n variables es[11] $VR(2,n) = 2^n$, y el número total de juntores enádicos es[11] $VR(2,2^n) = 2^{2^n}$. (Continúa en la actividad 19.9 [pág. 1158 de esta edición]). ■

En la lógica de juntores:

0. los dos juntores medádicos son *tautología* (⊤) y *contradicción* (⊥), cuyas tablas de verdad son

⊤	⊥
1	0

1. los cuatro juntores monádicos son *tautología* (⊤), *negador* (¬), *afirmador* (id) y *contradicción* (⊥), cuyas tablas de verdad son

p	⊤	$\neg p$	id$p$	⊥
1	1	0	1	0
0	1	1	0	0

2. los 16 juntores diádicos son *tautología* (⊤), *incompatibilizador* (|), *implicador (material)* (→), *negador (del argumento izquierdo)* ($\neg_0$), *replicador (material)* (←), *negador (del argumento derecho)* ($\neg_1$), *equivaledor* (↔), *negador conjunto* (↓), *disyuntor* (∨), *contravaledor* ($\veebar$), *afirmador (del argumento derecho)* (id_1), *desreplicador (material)* (↚), *afirmador (del argumento izquierdo)* (id_0), *desimplicador (material)*

[11] *Vid. infra* teorema 19.32 (pág. 1156 de esta edición).

($\nrightarrow$), *conjuntor* ($\wedge$) y *contradicción* ($\bot$), cuyas tablas de verdad son

p	q	$\top$	$p \mid q$	$p \to q$	$p \neg_0 q$	$p \leftarrow q$	$p \neg_1 q$	$p \leftrightarrow q$	$p \downarrow q$
1	1	1	0	1	0	1	0	1	0
1	0	1	1	0	0	1	1	0	0
0	1	1	1	1	1	0	0	0	0
0	0	1	1	1	1	1	1	1	1

p	q	$p \vee q$	$p \veebar q$	$p \,\mathrm{id}_1\, q$	$p \nleftarrow q$	$p \,\mathrm{id}_0\, q$	$p \nrightarrow q$	$p \wedge q$	$\bot$
1	1	1	0	1	0	1	0	1	0
1	0	1	1	0	0	1	1	0	0
0	1	1	1	1	1	0	0	0	0
0	0	0	0	0	0	0	0	0	0

Las estudiaremos en § 1.3 (págs. 77ss. de esta edición).

Observación 1.1.0.— Las parejas de juntores y sus negaciones son:

- tautología ($\top$), contradicción ($\bot$);
- afirmador (id), negador ($\neg$); igual como juntores diádicos:
  - afirmador del argumento izquierdo (id_0), negador del argumento izquierdo ($\neg_0$);
  - afirmador del argumento derecho (id_1), negador del argumento derecho ($\neg_1$);
- disyuntor ($\vee$), negador conjunto ($\downarrow$); (de aquí que sea frecuente designar este último por $\overline{\vee}$);
- conjuntor ($\wedge$), incompatibilizador ($|$); (de aquí que sea frecuente designar este último por $\overline{\wedge}$);
- implicador (material) ($\to$), desimplicador (material) ($\nrightarrow$);
- replicador (material) ($\leftarrow$), desreplicador (material) ($\nleftarrow$);
- equivaledor ($\leftrightarrow$), contravaledor ($\veebar$): (de aquí que sea frecuente designar el primero por $\overline{\veebar}$).

§ 1.2 Función proposicional

La expresión «x es divisible por 24» es una proposición verdadera o falsa según el valor de x; si, por ejemplo, x es múltiplo de 24, esto es, si x es 0, -24, 24, -48, 48. . ., entonces es verdadera, pero si x no es múltiplo de 24, es falsa. Diríamos, por ejemplo, que

$$P(x) \fallingdotseq x \text{ es divisible por } 24$$

es una *función proposicional* en el conjunto de los números enteros, $P : \mathbb{Z} \longrightarrow \{0, 1\}$. Resultaría entonces que para cada número entero n, $P(n)$ es una proposición; por ejemplo,

$$P(0) \coloneqq 0 \text{ es divisible por } 24,$$
$$P(1) \coloneqq 1 \text{ es divisible por } 24,$$

son ambas proposiciones, siendo $P(1)$ verdadera y $P(0)$ falsa.

Definición 1.9 (Función proposicional).— Decimos de una fórmula que es una *función proposicional* (o, sinónimamente, *función*, *matriz* o *forma enunciativa* [FREGE]) definida en un conjunto C de posibles sujetos si se transforma en una proposición para algún elemento de C. El subconjunto S de elementos de C que satisfacen la fórmula se denomina a veces *conjunto de verdad* de la fórmula (o, sinónimamente, *conjunto-solución* o *parte de C asociada* a la fórmula).

Ejemplo 71

Sea $A = \{n \in \mathbb{N} : n \text{ es un número impar menor que } 23\}$. Sean:

$$Px \coloneqq x \text{ es divisible por } 6,$$
$$Qx \coloneqq x \text{ es un número primo.}$$

¿Cuáles son los conjuntos de verdad de Px y Qx en A?

Resolución.— El conjunto de verdad P de Px en A es $P = \emptyset$; el de Qx en A es $Q = \{3, 5, 7, 11, 13, 17, 19\}$. ■

Observación 1.2.0.— Como tal función que es $P(x)$, al sujeto, ese elemento indefinido x de C, también es posible referirnos a él como el *argumento de la función proposicional* $P(x)$, de manera que podremos hablar de *función proposicional monoargumental*, *diargumental*, *triargumental*, ..., *n-argumental* o *poliargumental* (más de un argumento pero sin especificar su número).

Observación 1.2.1.— Como hemos visto, somos libres de usar paréntesis o no, es decir, de escribir $P(x, y)$ o Pxy para la misma función proposicional; en cualquier caso, se predica P de x e y.

Observación 1.2.2.— El avance sobre la lógica tradicional ha sido advertir que el esquema S es P no corresponde a todas las proposiciones e idear el concepto de función proposicional $P(s)$ donde P designa el verbo y s el sujeto. Es frecuente para facilitar el cálculo lógico, que $P(s)$ se sustituya por una sola letra p.

§ 1.3 Composición mediante conexión y su simbolización

De los cuatro juntores monádicos y 16 diádicos,

$$\mathcal{J} = \{\bot, \mathrm{id}, \neg, \top\} \cup \{\bot, \mathrm{id}_0, \mathrm{id}_1, \neg_0, \neg_1, \vee, \wedge, \veebar, \to, \leftarrow, \nrightarrow, \nleftarrow, \leftrightarrow, |, \downarrow, \top\},$$

algunos son habituales en nuestro lenguaje ordinario.

En este subcapítulo veremos el significado y el significante de estos enlaces entre proposiciones, reflexionaremos sobre cómo las conectamos, reuniremos diferentes expresiones en español que representan esas conexiones, presentaremos los símbolos que usaremos para designar los signos sentenciales conectivos y proporcionamos sus definiciones mediante sus tablas de verdad[12].

Ejemplo 72

0. Pensemos en las proposiciones simples:

$$p_0 \fallingdotseq \text{6174 es un conjunto},$$
$$q_0 \fallingdotseq \text{6174 es un número natural},$$

y en las siguientes proposiciones compuestas —que se han obtenido conectando/juntando las representadas por p_0 y q_0 mediante diferentes juntores (destacados en letra itálica)—:

$p_1 \fallingdotseq$ *Indiscutiblemente* 6174 es un número natural.

$p_2 \fallingdotseq$ 6174 *no* es un conjunto.

$p_3 \fallingdotseq$ 6174 es un conjunto *o* 6174 es un número natural.

$p_4 \fallingdotseq$ 6174 es un conjunto *y* 6174 es un número natural.

$p_5 \fallingdotseq$ *O bien* 6174 es un conjunto *o bien* 6174 es un número natural.

$p_6 \fallingdotseq$ *Si* 6174 es un conjunto, *entonces* 6174 es un número natural.

$p_7 \fallingdotseq$ 6174 es un conjunto *siempre que* 6174 sea un número natural.

$p_8 \fallingdotseq$ 6174 es un conjunto, *pero* 6174 *no* es un número natural.

$p_9 \fallingdotseq$ 6174 *no* es un conjunto, *pero* 6174 (*sí*) es un número natural.

$p_{10} \fallingdotseq$ Ser 6174 un conjunto *es equivalente a* ser 6174 un número natural.

$p_{11} \fallingdotseq$ Ser 6174 un conjunto *es incompatible con* ser 6174 un número natural.

$p_{12} \fallingdotseq$ *Ni* 6174 es un conjunto *ni* 6174 es un número natural.

[12] *Vid. supra* definición 1.2 (pág. 65 de esta edición).

1. y también en las funciones proposicionales:

$$Px \leftrightharpoons x \text{ es una de mis amistades,}$$
$$Qx \leftrightharpoons x \text{ dice siempre la verdad.}$$

Trataremos sobre ellas en los ejemplos siguientes.

En general, dependiendo del número de proposiciones simples componentes que intervengan en la composición, así será el orden de dicha composición. Entonces:

- una *composición medádica* es una composición de orden cero, esto es, no tiene ninguna proposición simple componente;
- una *composición monádica* es una composición de orden uno, es decir, tiene una proposición simple componente;
- una *composición diádica* es una composición de orden dos, o sea, tiene dos proposiciones simples componentes;
- una *composición triádica* es una composición de orden tres, a saber, tiene tres proposiciones simples componentes;
- una *composición de orden superior* tiene más de tres proposiciones simples componentes; por ejemplo, las composiciones tetrádicas, pentádicas, hexádicas, heptádicas, etc., tienen, respectivamente, tres, cuatro, cinco, seis, siete, etc., proposiciones simples componentes.

A continuación, reunimos diferentes expresiones en español para expresar estas composiciones y proporcionamos sus definiciones mediante sus tablas de verdad[13].

§ 1.3.0 Composiciones medádicas

Dos son las composiciones de orden cero: tautología y contradicción. En efecto, entre las diferentes agrupaciones de condiciones de verdad hay dos casos extremos: tautología y contradicción. Ambas son independientes de las proposiciones simples componentes.

Tautología

La tautología es verdadera siempre.

En español, expresiones tales como, por ejemplo, las siguientes, expresan la *tautología*.

- «p es p»,

[13] *Vid. supra* definición 1.2 (pág. 65 de esta edición).

- «p se identifica con p»,
- «p significa que p».

Designamos el juntor correspondiente a la tautología por $\top$.

Observación 1.3.0.— Es posible considerar la tautología actuando sobre una o más proposiciones, siendo $\top p$, $p \top q$, etc., proposiciones compuestas verdaderas independientemente de cómo sean sus proposiciones simples componentes. De este modo, resumimos las condiciones de verdad de la tautología en una disposición llamada tabla de verdad[14]. Por ejemplo, ésta es la tabla de verdad para una proposición atómica

p	$\top p$
1	1
0	1

en la que apreciamos cómo la tautología identifica una proposición consigo misma. Y ésta es la tabla de verdad para dos proposiciones simples componentes:

p	q	$p \top q$
1	1	1
1	0	1
0	1	1
0	0	1

Además de $\top$ también son frecuentes las designaciones 1, V y $\curlyvee$ (*verum*).

Contradicción

La contradicción es falsa siempre.

En español, expresiones tales como, por ejemplo, las siguientes, expresan la *contradicción*.

- «p no es p»,
- «p significa que es falso p».

Designamos el juntor correspondiente a la contradicción por $\bot$.

Observación 1.3.1.— Es posible considerar la contradicción actuando sobre una o más proposiciones, siendo $\bot p$, $p \bot q$, etc., proposiciones compuestas falsas independientemente de cómo sean sus proposiciones simples componentes. De este modo, para una proposición atómica, resumimos

[14] *Vid. supra* definición 1.2 (pág. 65 de esta edición).

las condiciones de verdad de la contradicción en la tabla de verdad

p	$\bot p$
1	0
0	0

en la que apreciamos cómo en la contradicción, una proposición se niega de sí misma. Y ésta es la tabla de verdad para dos proposiciones simples componentes:

p	q	$p \bot q$
1	1	0
1	0	0
0	1	0
0	0	0

Además de $\bot$ también son frecuentes las designaciones 0, F y $\curlywedge$ (*falsum*).

Observación 1.3.2.— En realidad, la tautología y la contradicción se clasifican como composiciones de cualquier orden.

§ 1.3.1 Composiciones monádicas

Dos son las composiciones nuevas de orden uno: negación y afirmación. Recordemos las observaciones anteriores; también son composiciones de orden uno la tautología y la contradicción —por eso hemos dicho «nuevas»—. En total, son cuatro las composiciones monádicas.

Negación

Una proposición compuesta *por negación* (o, sinónimamente, *por complementación*), es verdadera si, y sólo si, la proposición simple componente es falsa. Por tanto, es falsa si, y sólo si, la proposición simple componente es verdadera.

En latín, la negación de la proposición p es *non* p. En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de *negación* de p.

- «no p»,
- «es falso que suceda p»,
- «ni p»,
- «no es cierto de/que p»,
- «no es el caso de/que p»,
- «p, eso no es así»,
- «p, de eso nada»,
- «p, ¡venga ya!».

Observación 1.3.3.— Para recordar muchas más formas de la negación en español pudiésemos consultar Sanz Alonso [45].

El juntor correspondiente, llamado *negador*, lo designamos por $\neg$; la negación de p, por $\neg p$, que, como hemos dicho, es verdadera precisamente si p es falsa.

Resumimos las condiciones de verdad de la negación en la tabla de verdad

p	$\neg p$
1	0
0	1

en la que apreciamos que la negación asocia una proposición (p) a otra ($\neg p$) de valor de verdad diferente.

Ejemplo 73

Siendo:

$$p_0 \leftrightharpoons 6174 \text{ es un conjunto},$$
$$p_2 \leftrightharpoons 6174 \text{ \textit{no} es un conjunto},$$
$$Px \leftrightharpoons x \text{ es una de mis amistades},$$

nos preguntamos:

0., ¿es verdadera la proposición representada por p_2?, y

1., ¿qué proposición representa $\neg Px$?

Resolución.— Veamos:

- la proposición representada por p_2 es verdadera, ya que es «no p_0», es decir, p_2 es la negación de «6174 es un conjunto» que es su proposición simple componente y es falsa;
- $\neg Px$ representa la proposición «x no es una de mis amistades».[15] ■

Para expresar la negación de p, además de $\neg p$, también se usan las designaciones $\bar{p}$, $-p$ (Peano, 1886–1901) y $\sim p$ (es una n modificada muy utilizada en el siglo XIX, además de por Russell y Whitehead).

Observación 1.3.4.— La lógica clásica que estamos estudiando no trabaja con la *oposición*. «Esto es lo mejor» (proposición original) frente a «esto es lo peor» (proposición opuesta) frente a «esto no es lo mejor» (proposición negada). Pensar en términos opuestos es extremista (bueno/malo, fantástico/terrible, real/imaginario, blanco/negro), algo desgraciadamente frecuente en la política, donde los debates forman parte del pasado, de la historia. En la actualidad, todo queda en lo inmejorable de lo por mí elaborado frente a lo pésimo de lo por ti maquinado. En conjunción con nuestro sen-

[15] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).

tido común, el estudio de las *lógicas multivalentes*[16] y, quizás, en particular, de la *lógica borrosa*[17], pudiese ayudarnos a evitar los fundamentalismos, extremismos y autoengaños.

Afirmación

Una proposición compuesta *por afirmación* (o, sinónimamente, *por aserción* o *por identidad*), es verdadera si, y sólo si, la proposición simple componente es verdadera. Por tanto, es falsa si, y sólo si, la proposición simple componente es falsa.

En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de *afirmación* de p.

- «se satisface (que) p»,
- «es cierto (que) p»
- «ciertamente p»,
- «se tiene (que) p»,
- «sin duda p»,
- «es un hecho que p»,
- «indiscutiblemente p»,
- «como no puede ser de otro modo p».

Observación 1.3.5.— Para recordar algunas expresiones más de la afirmación en español pudiésemos consultar, por ejemplo, Santiago Barriendos, Polanco Martínez y Gras Manzano [46].

El juntor correspondiente, llamado *afirmador*, lo designamos por id; la afirmación de p, por id p, que, como hemos dicho, es verdadera precisamente si p es verdadera.

Resumimos las condiciones de verdad de la afirmación en la tabla de verdad

p	id p
1	1
0	0

que muestra cómo la afirmación asocia una proposición (p) a otra (id p) de igual valor de verdad.

[16] *Vid. infra* § 9 (pág. 516 de esta edición).
[17] *Cfr. v. gr.* León Rojas [1] (capítulo 4).

Ejemplo 74

Siendo:

$$q_0 \fallingdotseq 6174 \text{ es un número natural,}$$
$$p_1 \fallingdotseq \textit{Indiscutiblemente } 6174 \text{ es un número natural,}$$
$$Px \fallingdotseq x \text{ es una de mis amistades,}$$

nos preguntamos:

0., ¿es verdadera la proposición representada por p_1?, y

1., ¿qué proposición representa id Px?

Resolución.— Veamos:

- la proposición p_1 es verdadera, ya que es «indiscutiblemente q_0», es decir, p_1 es la afirmación de «6174 es un número natural» que es su proposición simple componente y es verdadera;
- la proposición id Px representa «indiscutiblemente x es una de mis amistades».[18] ■

Observación 1.3.6.— También pudiésemos haber dicho que id p es una abreviatura de $\neg\neg p$ y utilizar la tabla de verdad del negador para calcular la tabla de verdad de la afirmación.

Observación 1.3.7.— Según lo entiende el sentido común, atestar —y en el mismo sentido, jurar, dar fe, certificar— va más allá de afirmar o negar[19], sin embargo, a la hora de formalizar en lógica de primer orden tendrá la misma consideración.

§ 1.3.2 Composiciones diádicas. I

Cuando se componen dos proposiciones, hacemos una primera división:

- *composiciones conmutativas*, aquéllas que permiten cambiar el orden de las proposiciones sin alterar el significado de la proposición compuesta, y
- *composiciones no conmutativas*, aquéllas que si se altera el orden se altera el significado de la proposición resultante.

De las que vemos a continuación, son composiciones diádicas no conmutativas la implicación, la replicación, la desimplicación y la desreplicación[20]; las restantes son composiciones diádicas conmutativas.

[18] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).
[19] *Cfr. v. gr.* Díaz [47].
[20] Todas éstas las recogemos en § 1.3.3 (págs. 90ss. de esta edición).

Disyunción

Una proposición compuesta *por disyunción* (o, sinónimamente, *por alternativa* o *por adjunción* [LORENZEN] o, dicho con refuerzo, *por disyunción incluyente* [o *inclusiva*], esto es, sin excluir la verdad simultánea) es falsa si, y sólo si, las dos proposiciones simples componentes son falsas. Por lo tanto, es verdadera si, y sólo si, alguna de las proposiciones simples componentes es verdadera.

En latín, la disyunción de las proposiciones p y q es p *vel* q. En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de que puede suceder p, o bien q, o bien las dos.

- «p o/u q»,
- p, q, la una . . ., la otra . . . (, ambas . . .),
- bien p, bien q (, bien ambas)
- «necesariamente p o q (o ambas)»
- «ya p, ya q (, ya ambas)»,
- «al menos p, al menos q (, al menos ambas)»,
- «siquiera p, siquiera q (, siquiera ambas)»,
- «tan pronto p como q (como ambas)».

Observación 1.3.8.— Para recordar algunas expresiones más de la disyunción en español pudiésemos consultar LABRADOR GUTIÉRREZ [48].

El juntor correspondiente, llamado *disyuntor* (o, sinónimamente, *disyuntor incluyente* o *disyuntor inclusivo*[21]), lo designamos por $\vee$; la disyunción de p y q, por $p \vee q$ (RUSSELL y WHITEHEAD) que, como hemos dicho, es falsa cuando ambas son falsas y verdadera en los tres casos restantes. Los argumentos p y q de la disyunción, los llamamos *disyuntos*.

Resumimos las condiciones de verdad de la disyunción en la siguiente tabla de verdad:

p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0

[21] En vez del adjetivo «incluyente» o «inclusivo», se utiliza a veces *no-exclusivo*, expresión acuñada por COOLEY [49], y que ha sido usada posteriormente, entre otras personas, por QUINE.

Ejemplo 75

Siendo:

$$p_0 \coloneqq \text{6174 es un conjunto,}$$
$$q_0 \coloneqq \text{6174 es un número natural,}$$
$$p_3 \coloneqq \text{6174 es un conjunto } o \text{ 6174 es un número natural,}$$
$$Px \coloneqq x \text{ es una de mis amistades,}$$
$$Qx \coloneqq x \text{ dice siempre la verdad,}$$

nos preguntamos:

0., ¿es verdadera la proposición representada por p_3?, y

1., ¿qué proposición representa $Px \vee Qx$?

Resolución.— Veamos:

- la proposición p_3 es verdadera porque es «p_0 o q_0» y una de sus proposiciones simples componentes, a saber, «6174 es un número natural», es verdadera;
- la proposición $Px \vee Qx$ representa «x es una de mis amistades o dice siempre la verdad, o ambas cosas».[22] ■

Para expresar la disyunción de p y q, además de $p \vee q$, también se usa la designación $p + q$.

Inyección SQL

Para un uso malicioso de la disyunción pudiésemos buscar información sobre la inyección SQL (y sus contramedidas).*.

* *Vid. v. gr.* https://en.wikipedia.org/wiki/SQL_injection.

Conjunción

Una proposición compuesta *por conjunción* (o, sinónimamente, *por afirmación conjunta*), es verdadera si, y sólo si, las dos proposiciones simples componentes son verdaderas. Por lo tanto, es falsa si, y sólo si, alguna de las proposiciones simples componentes es falsa.

En latín, la conjunción de las proposiciones p y q es p *et* q. En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de que deben suceder p y q a la vez.

- «p e/y q»,
- «p, además de q»,

[22] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).

- «p, amén de q»,
- «p, junto con q»,
- «p, pero q»,
- «p, mas no $\neg q$»,
- «p; sin embargo q (o no $\neg q$)»,
- «p (o no $\neg p$); sin embargo q»,
- «p, aunque q»,
- «a pesar de (que) p, q»,
- «p, aun cuando q»,
- «p, aun si q»,
- «p, si bien q»,
- «p, mal que q»,
- «p, por más que q»,
- «p, siquiera sea q»,
- «p (o no $\neg p$), antes (o antes bien) q»,
- «p; por lo demás, q»,
- «p (o no $\neg p$), sino que q»,
- «p; con todo, q (o no $\neg q$)»,
- «p (o no $\neg p$); más bien, q»,
- «p (o no $\neg p$), fuera de (/excepto/salvo) q»,
- «p, menos $\neg q$»,
- «p; no obstante q»,
- «p, q»,
- «ambas a la par: p; q».

El juntor correspondiente, llamado *conjuntor* (o, sinónimamente, *conyuntor*), lo designamos por $\wedge$ (signo «cuña»); la conjunción de p y q, por $p \wedge q$, que, como hemos dicho, es verdadera cuando ambas son verdaderas y falsa en los tres casos restantes. Los argumentos p y q de la conjunción, los llamamos *conjuntos* (o, sinónimamente, *conyuntos*).

Resumimos las condiciones de verdad de la conjunción en la siguiente tabla de verdad:

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

Observación 1.3.9.— También pudiésemos haber dicho que $p \wedge q$ es una abreviatura de $\neg(\neg p \vee \neg q)$ y utilizar las tablas de verdad del negador y de la disyunción para calcular los valores anteriores —en este sentido hablaríamos de conjunción «material», de un mero cálculo de valores, independientemente del significado de p y q—.

Ejemplo 76

Siendo:

$$p_0 \fallingdotseq 6174 \text{ es un conjunto},$$
$$q_0 \fallingdotseq 6174 \text{ es un número natural},$$
$$p_4 \fallingdotseq 6174 \text{ es un conjunto } y \text{ 6174 es un número natural},$$
$$Px \fallingdotseq x \text{ es una de mis amistades},$$
$$Qx \fallingdotseq x \text{ dice siempre la verdad},$$

nos preguntamos:

0., ¿es verdadera la proposición representada por p_4?, y

1., ¿qué proposición representa $Px \wedge Qx$?

Resolución.— Veamos:

0. la proposición p_4 es falsa porque es «p_0 y q_0» y una de sus proposiciones simples componentes, a saber, «6174 es un conjunto», es falsa;

1. la proposición $Px \wedge Qx$ representa «x, además de ser una de mis amistades, dice siempre la verdad».[23] ■

Para expresar la conjunción de p y q, además de $p \wedge q$, también se usan las designaciones $p\&q$ (Hilbert, 1928), $p \cdot q$ o simplemente pq (Peano, 1886–1901, utilizada por Quine).

Observación 1.3.10.— $\{\neg, \vee, \wedge\}$ es una base de juntores[24] muy usada. Por ejemplo, para expresar una fórmula como una disyunción de cubos o como una conjunción de cláusulas, en forma normal disyuntiva (FND) —también llamada suma de productos— y en forma normal conjuntiva (FNC) —también llamada producto de sumas—, respectivamente[25]. En el caso de la disyunción, la expresión $p \vee q$ está en FND —disyunción de dos cubos— y en FNC —conjunción de una cláusula—. Para la conjunción sucede algo similar: la expresión $p \wedge q$ está en FND (disyunción de un cubo) y en FNC (conjunción de dos cláusulas).

Observación 1.3.11.— Con respecto a la observación anterior, añadir que otra expresión en FNC para $p \vee q$ es $(p \vee q) \wedge \top$ y que otra expresión en FND para $p \wedge q$ es $(p \wedge q) \vee \bot$ (basta comprobar la igualdad de sus tablas de verdad para demostrarlo).

[23] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).
[24] *Cfr. supra* § 0.23 (pág. 50 de esta edición) y *cfr. infra* § 1.15 (pág. 161 de esta edición).
[25] *Cfr. infra* § 3.1 (pág. 257 de esta edición).

Observación 1.3.12.— Con respecto a la confusión en la lengua natural entre la conjunción y la implicación, *vid. infra* § 1.3.21 (pág. 94 de esta edición).

Contravalencia

Una proposición compuesta *por contravalencia* (o, sinónimamente, *por disyunción excluyente* [o *exclusiva*] —exluyendo la verdad simultánea— o *por bisubstracción* [LORENZEN] o *por no equivalencia*) es verdadera si, y sólo si, sólo exactamente una de las dos proposiciones simples componentes es verdadera.

En latín, la contravalencia de p y q es p *aut* q. En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de una contravalencia, esto es, de una disyunción pero sin que puedan suceder las dos a la vez.

- «p vale contra q»,
- «p contravale q»,
- «p está en contravalencia con q»,
- «o p o q»,
- «o bien p o bien q»,
- «necesariamente p o q, pero no ambas».

El juntor correspondiente, llamado *contravaledor* (o, sinónimamente, *disyuntor excluyente* [o inclusivo]), lo designamos por $\veebar$; la contravalencia de p y q, por $p \veebar q$, que, como hemos dicho, es verdadera cuando una es verdadera y la otra falsa, y falsa en los dos casos restantes.

Resumimos las condiciones de verdad de la contravalencia en la tabla de verdad

p	q	$p \veebar q$
1	1	0
1	0	1
0	1	1
0	0	0

Observación 1.3.13.— También pudiésemos haber dicho que $p \veebar q$ es una abreviatura bien de $\neg(\neg p \vee q) \vee \neg(p \vee \neg q)$, bien de $\neg(p \wedge q) \wedge \neg(\neg p \wedge \neg q)$, y utilizar las tablas de verdad del negador y de la disyunción en el primer caso y del negador y de la conjunción en el segundo; igualmente, en línea con la «materialidad» de un simple cálculo y no con la significación de p y q.

Ejemplo 77

0. «Su hija nació en junio o julio» es una contravalencia, pues no pudo nacer en ambos meses.

1. La expresión «iré con él o con ella» puede que nos resulte ambigüa, pues podría ir con los dos; pero si nuestra idea es ir sólo con uno de los dos pudiésemos decir: «iré, o bien con él, o bien con ella».

Ejemplo 78

Siendo:

$p_0 \fallingdotseq$ 6174 es un conjunto,

$q_0 \fallingdotseq$ 6174 es un número natural,

$p_5 \fallingdotseq$ *O bien* 6174 es un conjunto *o bien* 6174 es un número natural,

$Px \fallingdotseq$ x es una de mis amistades,

$Qx \fallingdotseq$ x dice siempre la verdad,

nos preguntamos:

0., ¿es verdadera la proposición representada por p_5?, y

1., ¿qué proposición representa $Px \veebar Qx$?

Resolución.— Veamos:

- la proposición representada por p_5 es una contravalencia «o bien p_0 o bien q_0» (a pesar de que, como veremos más adelante, un número natural puede definirse como un conjunto).
- $Px \veebar Qx$ representa la proposición «o bien x es una de mis amistades o bien x dice siempre la verdad».[26] ■

Para expresar la contravalencia de p y q, además de $p \veebar q$, también se usan las designaciones $p \circledvee q$, $p \omega q$, $p \oplus q$, $p >\!\!-\!\!< q$, $p \not\leftrightarrow q$ y $p \not\equiv q$.[27]

Observación 1.3.14.— La contravalencia $p \veebar q$ suele expresarse también como una disyunción de cubos y como una conjunción de cláusulas, en forma normal disyuntiva (FND) y en forma normal conjuntiva (FNC), respectivamente[28]. En efecto:

0. $(p \wedge \neg q) \vee (\neg p \wedge q)$; (FND)
1. $(\neg p \vee \neg q) \wedge (p \vee q)$. (FNC)

[26] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).

[27] Los estoicos (Zenón de Citio, Crisipo de Solos, etc.), en su etapa más antigua, desde el 300 a. C., investigaron la negación, conjunción y disyunción. Petrus Hispanus, John Duns Scotus, George Boole (1847) y Friedrich Wilhelm Karl Ernst Schröder (1877) continuaron tal estudio.

[28] *Cfr. infra* § 3.1 (pág. 257 de esta edición).

Basta comprobar la igualdad de sus tablas de verdad para demostrarlo.

Aplicación de la contravalencia: intercambio de valores de variables

En ocasiones ocurre que tenemos que intercambiar el valor de dos variables, digamos x e y, para lo que pudiésemos usar una variable temporal, digamos t,

```
t ↤ x;
x ↤ y;
y ↤ t;
```

si bien es innecesario usar tal artificio, pues la cuestión se resuelve usando la contravalencia tres veces —proceso válido para cualquier patrón de bits y, por tanto, independiente del tipo de datos de las variables—, así:

```
x ↤ x xor y;
y ↤ y xor x;
x ↤ x xor y;
```

Por ejemplo,

Pseudocódigo	Valor de x	Valor de y
	2	3
`x ↤ x xor y (010 xor 011 = 001)`	1	3
`y ↤ y xor x (011 xor 001 = 010)`	1	2
`x ↤ x xor y (001 xor 010 = 011)`	3	2

§ 1.3.3 Composiciones diádicas. II

Como dijimos, la implicación, la replicación, la desimplicación y la desreplicación son composiciones no conmutativas. La equivalencia sí es conmutativa.

Implicación

Una proposición compuesta *por implicación (material)*, también llamada *proposición condicional* o *subjunción* (Lorenzen), es falsa si, y sólo si, la proposición simple componente a la izquierda del juntor —proposición *antecedente/condicionante/implicante*— es verdadera y la proposición simple componente a la derecha del juntor —proposición *consecuente/condicionada/implicada*— es falsa. Por tanto, es verdadera en cualquiera de los otros tres casos.

En latín, que p implique q es p *seq* q. En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de una deducción, «de afirmar que sucede p, se deduce la afirmación de que sucede q», es decir, entendemos p *seq* q como *non* p *vel* q.

- «p implica q»,
- «si p, entonces (necesariamente) q»,
- «p es (una condición) suficiente para q»,
- «p a condición de que q»,
- «p, con tal (de) que q»,
- «p sólo si q»,
- «sólo p si q»,
- «p; debido a ello, q»,
- «como p, (entonces) q»,
- «q, en el supuesto de que p»,
- «q (en el) caso de que p»,
- «q como p»,
- «comoquiera que p, (entonces) q»,
- «cuando p, (entonces) q»,
- «q cuando p»,
- «en vista de/visto que p, (entonces) q»,
- «por razón de que p, (entonces) q»,
- «p es la razón por la que q»,
- «p, por esta razón, q»,
- «p, por eso q»,
- «porque p, (entonces) q»,
- «puesto que p, (entonces) q»,
- «siempre que p, (entonces) q»,
- «q, siempre que p»,
- «ya que p, (entonces) q»,
- «no hay p sin q»,
- «no p a menos que q»,
- «ningún p sin q»,
- «p es replicada por q».

Así entendida, se trata de la *implicación material* o *condicional material*, independiente de los significados de las proposiciones que p y q representan[29].

El juntor correspondiente, llamado *implicador (material)* (o, sinónimamente, *condicional* o *condicionador*), lo designamos por $\rightarrow$; el hecho de p implicar q, por $p \rightarrow q$, proposición que, como hemos dicho, es falsa cuando el antecedente es verdadero y el consecuente falso, y verdadera en los tres casos restantes.

Como también hemos mencionado, llamamos a p, *antecedente* o *implicante* (de q) o *condición suficiente* (para que ocurra q) y a q, *consecuente* o *implicada* (de p) o *condición necesaria* (para que ocurra p) (*conditio sine qua non*, esto es, condición sin la cual no); en lingüística, a la proposición condicional, p, se le da el nombre de *prótasis* y a la proposición principal, q, el de *apódosis*.

[29] Un ejemplo de concepción alternativa es la de *implicación significante* en la *lógica de significaciones* que obliga a que una significación del consecuente sea una de las del antecedente y esta significación común sea transitiva (*cfr. v. gr.* Piaget y García [50]).

Resumimos las condiciones de verdad de la implicación en la tabla de verdad

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

Observación 1.3.15.— También pudiésemos haber dicho que $p \to q$ es una abreviatura de $\neg p \vee q$, y utilizar las tablas de verdad del negador y de la disyunción, o bien una abreviatura de $\neg(p \wedge \neg q)$, y utilizar las tablas de verdad del negador y de la conjunción.

Ejemplo 79

Siendo:

$p_0 \risingdotseq$ 6174 es un conjunto,

$q_0 \risingdotseq$ 6174 es un número natural,

$p_6 \risingdotseq$ *Si* 6174 es un conjunto, *entonces* 6174 es un número natural,

$Px \risingdotseq x$ es una de mis amistades,

$Qx \risingdotseq x$ dice siempre la verdad,

nos preguntamos:

0., ¿es verdadera la proposición representada por p_6?, y

1., ¿qué proposición representa $Px \to Qx$?

Resolución.— Veamos:

- la proposición representada por p_6 es verdadera porque es «p_0 implica q_0» y la proposición simple antecedente, a saber, «6174 es un conjunto», en un sentido elemental, es falsa;
- $Px \to Qx$ representa la proposición «si x es una de mis amistades, entonces dice siempre la verdad».[30] ■

También se usan las designaciones $p \supset q$ (GERGONNE, 1816)[31] y $p \leq q$.

[30] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).

[31] Parece ser que fue FILÓN de Megara —*vid. v. gr.* https://es.wikipedia.org/wiki/Filón_de_Megara— quien propuso el uso del implicador, siendo Friedrich Ludwig Gottlob FREGE (1879) y Charles Sanders PEIRCE (1885) quienes lo reintrodujeron en la formalización actual de la lógica.

Observación 1.3.16.— Es posible también expresar la implicación $p \to q$ como una disyunción de cubos y como una conjunción de cláusulas, en forma normal disyuntiva (FND) y en forma normal conjuntiva (FNC), respectivamente[32]. En efecto:

0. $\neg p \vee q$ (FND)

1. $\neg p \vee q$ (FNC)

Basta comprobar la igualdad de sus tablas de verdad para demostrarlo.

Observación 1.3.17.— Es posible expresar fácilmente $\neg p \vee q$ como una conjunción, concretamente por $(\neg p \vee q) \wedge \top$ (de nuevo, basta comprobar la igualdad de sus tablas de verdad para demostrar que es así).

Observación 1.3.18.— En algunos textos se advierte de que, formalmente, al expresarnos en lógica, quizás debiésemos tener cuidado con no confundir «si-entonces» con «implica»; según esos textos, la primera expresión pertenece al lenguaje objeto (nivel 0), mientras que la segunda, al metalenguaje (nivel 1).

Observación 1.3.19.— Más adelante, estudiaremos la *implicación lógica*[33], que designaremos por el símbolo $\vDash$, de forma que *la expresión* $p \vDash q$ *representa una argumentación válida* —el hecho de ser q consecuencia lógica de p— y cuya traducción al español viene dada típicamente por conjunciones y locuciones ilativas y consecutivas, es decir, por expresiones tales como, por ejemplo, las siguientes.

- «p, así q»,
- «p, así (es) que q»,
- «p, conque q»,
- «(sólo) con que p, q»,
- «con p, q»,
- «p, de aquí/ahí que q»,
- «p, de forma/manera/modo que q»,
- «p, en conclusión q»,
- «p, en consecuencia q»,
- «p, luego q»,
- «p; q, pues»,
- «dado p, q»,
- «p da lugar a q»,
- «de p, se sigue q»,
- «p, por consiguiente q»,
- «p, consiguientemente/consecuentemente q»,
- «p, por lo que q»,
- «p, por (lo) tanto q»,
- «de p, se concluye/deduce q»,
- «de p, se infiere q».

[32] *Cfr. infra* § 3.1 (pág. 257 de esta edición).
[33] *Cfr. infra* § 1.10 (pág. 145 de esta edición]).

Como veremos, la implicación lógica pertenece al metalenguaje (nivel 1) y su traducción al lenguaje objeto (nivel 0) es la implicación material. Por otro lado, como hemos dicho, la implicación lógica indica la validez de una argumentación, por lo que si lo que perseguimos es una representación de esta última en el lenguaje objeto, será la implicación material la que indique la verdad de la expresión resultante.

Observación 1.3.20.— (En la que seguimos a Lázaro Carreter y Tusón Valls [51]).

En la lengua española, la prótasis puede presentarse en varios modos: la *prótasis en imperativo* («Hágalo usted y no lo haré yo», «Hágalo: verá como yo no lo hago» [Si lo hace usted, entonces no lo haré yo]), la *prótasis en infinitivo* («De hacerlo usted, no lo haré yo», «Yo lo hubiese hecho, de no hacerlo usted»), la *prótasis en gerundio* («Haciéndolo usted, yo no lo hago»), la *prótasis en participio* («Esto, hecho por usted, resulta ser una mejor solución»), la *prótasis elíptica* («Yo no lo haría mejor» [Si lo hiciese yo...]).

Por otra parte, la riqueza de la lengua española hace que gocemos de una vasta variedad de expresiones para la condición. Más ejemplos: «Con ese artefacto haría los cálculos más rápido»; «Increíblemente, con que hubiese un computador más en la red, se reduciría el tiempo de cómputo en más de la mitad»; «Los ponemos a calcular y avanzamos»; «Que pudiésemos disponer de un computador cuántico, ya vería usted»; «No se conforme con no ser feliz».

Observación 1.3.21.— Debemos tener cuidado también con la traducción inversa de expresiones que incluyan «y», por ejemplo, éste que sigue parece que no presenta dificultad:

- «Entre tú y yo lo hacemos» podría traducirse como «Tú lo haces y yo lo hago», esto es, como la forma lógica $p \wedge q$ (puesto que aparentemente 'y' significa sólo adición).

Sin embargo, en los tres siguientes, a modo de ejemplos, quien siguiese defendiendo la conjunción estaría hablando de una conjunción, como mínimo, no conmutativa (signifique esto lo que signifique):

- «Acertó y ganó» podría traducirse como «Acertó, por consiguiente, ganó», esto es, como la forma lógica $p \rightarrow q$ (puesto que aparentemente 'y' significa 'por consiguiente', por lo que parece inaceptable cambiar el orden de los sucesos 'acertar' y 'ganar').
- «Llegamos a casa y cenamos en la tranquilidad del hogar», podría traducirse como «Llegamos a casa y después cenamos en la tranquilidad del hogar», esto es, como la forma lógica $p \rightarrow q$ (puesto que aparentemente 'y' significa 'y después', por lo que parece inaceptable cambiar el orden de los sucesos 'llegar a casa' y 'cenar en la tranquilidad del hogar').
- «Se esforzó mucho y lo consiguió» podría traducirse como «Se esforzó tanto que (como consecuencia) lo consiguió», esto es, como la forma lógica $p \rightarrow q$ (puesto que aparentemente 'y' significa 'como consecuencia', por lo que también parece inaceptable cambiar el orden de los sucesos 'esforzarse mucho' y 'conseguirlo').

Observación 1.3.22.— Formalmente, $Px \rightarrow Qx$ es un *condicional generalizado*, en el sentido de que al recorrer x un universo de interpretación dado, genera una colección de condicionales materiales, tantos como entidades haya en dicho universo.

Observación 1.3.23.— En estas notas no estudiamos *condicionales contrafácticos*, esto es, en modo subjuntivo, por ejemplo: «Si x hubiese sido una posibilidad, entonces no habríamos elegido y», si bien, recientes e innovadoras líneas de investigación los sitúan como los últimos explicadores de la naturaleza de la realidad[34].

Observación 1.3.24.— Tampoco abordamos las *presuposiciones*, estudiadas por la semántica. Por ejemplo, en «Sigo aquí» hay una proposición presupuesta, «Yo estaba aquí», cuya verdad conlleva la verdad de aquélla.

Observación 1.3.25.— Asimismo no son materia de estas notas las *implicaturas*, ampliamente estudiadas por la pragmática[35]. Por ejemplo: en «Hasta yo lo escalé» hay una implicatura convencional de sorpresa ante el hecho de que yo lo haya escalado; en la afirmación «María tiene dos carreras» hay una implicatura conversacional de exactitud, casi nadie interpretará que María tiene al menos dos carreras, al contrario, la mayoría interpretaremos que María tiene «exactamente» dos carreras.

Replicación (implicación recíproca)

Una proposición compuesta *por replicación* (o, sinónimamente, *por implicación recíproca*) (también llamada *subjunción conversa* por LORENZEN) es falsa si, y sólo si, la proposición simple componente a la derecha del juntor es verdadera y la proposición simple componente a la izquierda del juntor es falsa. Por tanto, es verdadera en cualquiera de los otros tres casos.

En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de una deducción, «de afirmar que sucede q se deduce la afirmación de que sucede p».

- «p replica q»,
- «sólo si p, entonces (posiblemente) q»,
- «p es (una condición) necesaria para q»,
- «p si q»,
- «p cuando q»,
- «p, en vista de/visto que q»,
- «p, por razón de que q»,
- p porque q,
- p pues q,
- p puesto que q,
- «p siempre que q»,
- «p ya que q»,
- «sin p, no hay q»,
- «p es la causa de q»,

[34] *Cfr. v. gr.* PEARL [52]; PEARL y MACKENZIE [53], y MARLETTO [54].
[35] *Cfr. v. gr.* REYES [38].

- «a no ser que p, no q»,
- «p es implicada por q».

El juntor correspondiente, llamado *replicador* (o, sinónimamente, *implicador recíproco* o *condicionador recíproco*) lo designamos por $\leftarrow$; el hecho de p ser implicado por q, por $p \leftarrow q$, proposición que, como hemos dicho, es falsa cuando el p es falsa y q es verdadera, y verdadera en los tres casos restantes.

La proposición p, la llamamos *replicante*, y la proposición q, *replicada*.

Resumimos las condiciones de verdad de la replicación en la tabla de verdad

p	q	$p \leftarrow q$
1	1	1
1	0	1
0	1	0
0	0	1

Observación 1.3.26.— También pudiésemos haber dicho que $p \leftarrow q$ es una abreviatura de $p \vee \neg q$, y utilizar las tablas de verdad del negador y de la disyunción, o bien una abreviatura de $\neg(\neg p \wedge q)$, y utilizar las tablas de verdad del negador y de la conjunción.

Ejemplo 80

Siendo:

$p_0 \fallingdotseq$ 6174 es un conjunto,

$q_0 \fallingdotseq$ 6174 es un número natural,

$p_7 \fallingdotseq$ 6174 es un conjunto *siempre que* 6174 sea un número natural,

$Px \fallingdotseq x$ es una de mis amistades,

$Qx \fallingdotseq x$ dice siempre la verdad,

nos preguntamos:

0., ¿es verdadera la proposición representada por p_7?, y

1., ¿qué proposición representa $Px \leftarrow Qx$?

Resolución.— Veamos:

- la proposición representada por p_7 es falsa porque es «p_0 replica q_0» y la proposición simple replicante, a saber, «6174 es un conjunto», en un sentido elemental, es falsa y la proposición simple replicada, verdadera;

- $Px \leftarrow Qx$ representa la proposición «x es una de mis amistades siempre que diga siempre la verdad».[36] ■

Para expresar que p replica q, además de $p \leftarrow q$, también se usan las designaciones $p \subset q$ y $p \geq q$.

Observación 1.3.27.— Es posible expresar la replicación $p \leftarrow q$ como una disyunción de cubos y como una conjunción de cláusulas, en forma normal disyuntiva (FND) y en forma normal conjuntiva (FNC), respectivamente[37]. En efecto:

0. $p \vee \neg q$ (FND)

1. $p \vee \neg q$ (FNC)

Basta comprobar la igualdad de sus tablas de verdad para demostrarlo.

Observación 1.3.28.— Es posible expresar fácilmente $p \vee \neg q$ como una conjunción, concretamente por $(p \vee \neg q) \wedge \top$ (de nuevo, basta comprobar la igualdad de sus tablas de verdad para demostrar que es así).

Observación 1.3.29.— En algunos textos se advierte de que, formalmente, al expresarnos en lógica, quizás debiésemos tener cuidado con no confundir «sólo si-entonces» con «replica» (o «es implicada por»); según esos textos, la primera expresión pertenecería al lenguaje objeto (nivel 0), mientras que la segunda, al metalenguaje (nivel 1).

Observación 1.3.30.— Análogamente a la implicación lógica[38], estudiaremos más adelante la *replicación lógica*[39], la que designaremos por el símbolo $\dashv$, de forma que *la expresión* $p \dashv q$ *representa una argumentación válida* —el hecho de ser p consecuencia de q— y cuya traducción al español viene dada típicamente por conjunciones y locuciones ilativas y consecutivas, es decir, por expresiones tales como, por ejemplo,

- «p es conclusión de q»,
- «p es consecuencia de q»,
- «p se ha concluido/deducido de q».

Como veremos, la replicación lógica pertenece al metalenguaje (nivel 1) y su traducción al lenguaje objeto (nivel 0) es la replicación material. Por otro lado, como hemos dicho, la replicación

[36] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).
[37] *Cfr. infra* § 3.1 (pág. 257 de esta edición).
[38] *Cfr. supra* observación 1.3.19 (pág. 93 de esta edición).
[39] *Cfr. infra* § 1.13 (pág. 156 de esta edición).

lógica indica la validez de una argumentación, por lo que si lo que perseguimos es una representación de ésta en el lenguaje objeto con la replicación material, sepamos que la expresión resultante será verdadera.

Desimplicación (negación de la implicación)

Una proposición compuesta *por desimplicación* (o, sinónimamente, *por no implicación* o *inhibición* o *desigualdad propia*) es verdadera si, y sólo si, la proposición simple componente a la izquierda del juntor es verdadera y la proposición simple componente a la derecha del juntor es falsa. Por tanto, es falsa en cualquiera de los otros tres casos.

En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de una desimplicación, de que p no implica q porque puede suceder p y no suceder q.

- «p no implica q»,
- «p y no q»,
- «p, no q»,
- «p, además de no q»,
- «p, aunque no q»,
- «p, pero no q»,
- «p, sin embargo no q»,
- «p, mas no q»,
- «p menos q»,
- «p sin q»,
- «p, por más que no q».

Actividad 1.6

Negar una implicación no es sencillo. Muchas personas niegan «si p, entonces q» diciendo «si p, entonces no q». ¿Tienen razón o pudiésemos proporcionar un ejemplo que les convenciese de que no es así?

El juntor correspondiente, que llamamos *desimplicador*, lo designamos por $\nrightarrow$; el hecho de q no ser implicado por p, por $p \nrightarrow q$, proposición que, como hemos dicho, es verdadera cuando p es verdadera y q es falsa, y falsa en los tres casos restantes.

Resumimos las condiciones de verdad de la no implicación en la tabla de verdad

p	q	$p \nrightarrow q$
1	1	0
1	0	1
0	1	0
0	0	0

Observación 1.3.31.— También pudiésemos haber dicho que $p \nrightarrow q$ es una abreviatura de $\neg(\neg p \vee q)$, y utilizar las tablas de verdad del negador y de la disyunción, o bien una abreviatura de $(p \wedge \neg q)$, y utilizar las tablas de verdad del negador y de la conjunción.

Ejemplo 81

Siendo:

$$p_0 \risingdotseq 6174 \text{ es un conjunto},$$
$$q_0 \risingdotseq 6174 \text{ es un número natural},$$
$$p_8 \risingdotseq 6174 \text{ es un conjunto, } \textit{pero } 6174 \textit{ no} \text{ es un número natural},$$
$$Px \risingdotseq x \text{ es una de mis amistades},$$
$$Qx \risingdotseq x \text{ dice siempre la verdad},$$

nos preguntamos:

0., ¿es verdadera la proposición representada por p_8?, y

1., ¿qué proposición representa $Px \nrightarrow Qx$?

Resolución.— Veamos:

- la proposición representada por p_8 es falsa porque es «p_0 y no q_0» y la proposición simple a la izquierda, a saber, «6174 es un conjunto», en un sentido elemental, es falsa;
- $Px \nrightarrow Qx$ representa la proposición «x es una de mis amistades, sin embargo no dice siempre la verdad».[40] ■

Para expresar que p no implica q, además de $p \nrightarrow q$, también se usan las designaciones $p \bar{\rightarrow} q$, $p \leftarrowtail q$, $p > q$ o exageradamente $\not\to$.

Observación 1.3.32.— Es posible expresar la desimplicación $p \nrightarrow q$ como una disyunción de cubos y como una conjunción de cláusulas, en forma normal disyuntiva (FND) (una disyunción de un cubo) y en forma normal conjuntiva (FNC) (una conjunción de dos cláusulas), respectivamente[41]. En efecto:

0. $p \wedge \neg q$ (FND)

1. $p \wedge \neg q$ (FNC)

Basta comprobar la igualdad de sus tablas de verdad para demostrarlo.

[40] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).
[41] *Cfr. infra* § 3.1 (pág. 257 de esta edición).

Observación 1.3.33.— Es posible expresar fácilmente $p \wedge \neg q$ como una disyunción, concretamente por $(p \wedge \neg q) \vee \bot$ (de nuevo, basta comprobar la igualdad de sus tablas de verdad para demostrar que es así).

Desreplicación (negación de la replicación)

Una proposición compuesta *por desreplicación* (o, sinónimamente, *por no replicación* o *por inhibición* o *por desigualdad propia*), es verdadera si, y sólo si, la proposición simple componente a la derecha del juntor es verdadera y la proposición simple componente a la izquierda del juntor es falsa. Por tanto, es falsa en cualquiera de los otros tres casos.

En español, locuciones como, por ejemplo, las siguientes, expresan la idea de la negación de la replicación, de que p no replica q porque puede no suceder p y suceder q.

- «p no replica q»,
- «no p y q»,
- «no p, además de q»,
- «no p, aunque q»,
- «aunque no p, q»,
- «no p, pero q»,
- «no p, sin embargo q»,
- «no p, mas q»,
- «no p, q»,

El juntor correspondiente, que llamamos *desreplicador*, lo designamos por $\nleftarrow$ (o, sinónimamente, $\not\leftarrow$); el hecho de p no ser implicado por q, por $p \nleftarrow q$, proposición que, como hemos dicho, es verdadera cuando q es verdadera y p es falsa, y falsa en los tres casos restantes.

Resumimos las condiciones de verdad de la no replicación en la tabla de verdad

p	q	$p \nleftarrow q$
1	1	0
1	0	0
0	1	1
0	0	0

Observación 1.3.34.— También pudiésemos haber dicho que $p \nleftarrow q$ es una abreviatura de $\neg(p \vee \neg q)$, y utilizar las tablas de verdad del negador y de la disyunción, o bien una abreviatura de $\neg p \wedge q$, y utilizar las tablas de verdad del negador y de la conjunción.

Ejemplo 82

Siendo:

$$p_0 \fallingdotseq 6174 \text{ es un conjunto},$$
$$q_0 \fallingdotseq 6174 \text{ es un número natural},$$
$$p_9 \fallingdotseq 6174 \textit{ no} \text{ es un conjunto, } \textit{pero} \text{ 6174 (}\textit{sí}\text{) es un número natural},$$
$$Px \fallingdotseq x \text{ es una de mis amistades},$$
$$Qx \fallingdotseq x \text{ dice siempre la verdad},$$

nos preguntamos:

0., ¿es verdadera la proposición representada por p_9?, y

1., ¿qué proposición representa $Px \nleftarrow Qx$?

Resolución.— Veamos:

- la proposición representada por p_9 es verdadera porque es «no p_0 y q_0» y p_0, esto es, «6174 es un conjunto», en un sentido elemental, es falsa y p_1, es decir, «6174 es un número natural», es verdadera;
- $Px \nleftarrow Qx$ representa la proposición «x no es una de mis amistades, sin embargo dice siempre la verdad».[42] ■

Para expresar que p no replica q, además de $p \nleftarrow q$, también se usan las designaciones $p \mapsto q$ y $p < q$.

Observación 1.3.35.— La desreplicación $p \nleftarrow q$ puede expresarse también como una disyunción de cubos y como una conjunción de cláusulas, la forma normal disyuntiva (FND) y la forma normal conjuntiva (FNC), respectivamente[43]. En efecto:

0. $\neg p \wedge q$, (FND)
1. $\neg p \wedge q$. (FNC)

Basta comprobar la igualdad de sus tablas de verdad para demostrarlo.

Observación 1.3.36.— Es posible expresar fácilmente $\neg p \wedge q$ como una disyunción, concretamente por $(\neg p \wedge q) \vee \bot$ (de nuevo, basta comprobar la igualdad de sus tablas de verdad para demostrar que es así).

[42] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).
[43] *Cfr. infra* § 3.1 (pág. 257 de esta edición).

Equivalencia (negación de la contravalencia)

Una proposición compuesta *por equivalencia* (o, sinónimamente, *por coimplicación* o *por biimplicación*) (*material*) (también llamada *proposición bicondicional* y *bisubjunción* [LORENZEN]) es verdadera si, y sólo si, las dos proposiciones simples componentes son ambos verdaderas o ambos falsas. Por tanto, es falsa si, y sólo si, una de las proposiciones simples componentes es verdadera y la otra falsa.

En latín, la coimplicación de p y q se escribe p *aeq* q. En español, expresiones tales como, por ejemplo, las siguientes, expresan la idea de una doble condición.

- «p equivale a q»,
- «p precisamente si q»,
- «si, y sólo si, p, q»,
- «si, y sólo si, p, entonces q»,
- «p si, y sólo si, q» (abreviadamente, sólo en ámbitos formales concretos, «p sii q» o «p ssi q»),
- «p es verdad si, y sólo si, q es verdad»,
- «p cuando, y sólo cuando, q»,
- «p es condición necesaria y suficiente para q»,
- «p y q se implican mutuamente»,
- «si p es verdad, q es verdad, y si p es falso, q es falso».

El juntor correspondiente, llamado *equivaledor* (o, sinónimamente, *coimplicador*, *biimplicador* o *bicondicionador*) se nota $\leftrightarrow$, la equivalencia de p y q se nota $p \leftrightarrow q$, proposición que, como hemos dicho, es verdadera cuando y sólo cuando ambas tienen el mismo valor de verdad.

Resumimos las condiciones de verdad de la equivalencia (material) en la tabla de verdad

p	q	$p \leftrightarrow q$
1	1	1
1	0	0
0	1	0
0	0	1

Observación 1.3.37.— También pudiésemos haber dicho que $p \leftrightarrow q$ es una abreviatura de $\neg(p \vee q) \vee \neg(\neg p \vee \neg q)$, y utilizar las tablas de verdad del negador y de la disyunción, o bien una abreviatura de $\neg(p \wedge \neg q) \wedge \neg(\neg p \wedge q)$, y utilizar las tablas de verdad del negador y de la conjunción.

Ejemplo 83

Siendo:

$p_0 \risingdotseq$ 6174 es un conjunto,

$q_0 \risingdotseq$ 6174 es un número natural,

$p_{10} \risingdotseq$ Ser 6174 un conjunto *es equivalente a* ser 6174 un número natural,

$Px \risingdotseq x$ es una de mis amistades,

$Qx \risingdotseq x$ dice siempre la verdad,

nos preguntamos:

0., ¿es verdadera la proposición representada por p_{10}?, y

1., ¿qué proposición representa $Px \leftrightarrow Qx$?

Resolución.— Veamos:

- la proposición representada por p_{10} es falsa porque es «p_0 es equivalente a q_0» y la proposición simple componente «6174 es un conjunto», en un sentido elemental, es falsa y la proposición simple componente «6174 es un número natural» es verdadera; la proposición «p_0 es equivalente a q_0» tiene el mismo significado que «(si p_0, entonces q_0) y (si q_0, entonces p_0)»;
- $Px \leftrightarrow Qx$ representa la proposición «x es una de mis amistades precisamente si dice siempre la verdad».[44] ■

Para expresar la equivalencia de p y q, además de $p \leftrightarrow q$, también se usan las designaciones $p \overline{\veebar} q$ (negación de la contravalencia) y $p \equiv q$ (si bien ésta con sumo cuidado, pues puede ser confundida fácilmente con su uso metalingüístico).

Observación 1.3.38.— Es posible expresar la equivalencia $p \leftrightarrow q$ como una disyunción de cubos y como una conjunción de cláusulas, en forma normal disyuntiva (FND) y en forma normal conjuntiva (FNC), respectivamente[45]. En efecto:

0. $(p \wedge q) \vee (\neg p \wedge \neg q)$ (FND)
1. $(p \vee \neg q) \wedge (\neg p \vee q)$ (FNC)

Basta comprobar la igualdad de sus tablas de verdad para demostrarlo.

Observación 1.3.39.— En algunos textos se advierte de que, formalmente, al expresarnos en lógica, debiésemos tener cuidado con no confundir «si, y sólo si,» con «ser equivalente a»; según esos

[44] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).
[45] *Cfr. infra* § 3.1 (pág. 257 de esta edición).

textos, la primera expresión pertenece al lenguaje objeto (nivel 0), mientras que la segunda, al metalenguaje (nivel 1).

Observación 1.3.40.— En el lenguaje ordinario también se usa una estructura condicional, por ejemplo, «si Noche Buena es jueves, Navidad es viernes». Sin embargo, en este caso, supuesto el mismo año, se da la equivalencia, pues también es cierto que «si Navidad es viernes, Noche Buena es jueves». Formalizaríamos con $p \leftrightarrow q$, pues más que aparentemente ésa es la intención.

Incompatibilidad (negación de la conjunción)

Una proposición compuesta *por incompatibilidad* (o, sinónimamente, *por exclusión*, *por conjunción opuesta* o *por negación disyunta*[46]) es falsa si, y sólo si, ambas proposiciones simples componentes son verdaderas. Por tanto, es verdadera en cualquiera de los otros tres casos.

En español, expresiones tales como, por ejemplo, las siguientes, expresan la *incompatibilidad* de p y q, su *negación disyunta*.

- «no p o no q» (el o es incluyente),
- «p y q son incompatibles».

El juntor correspondiente, llamado *incompatibilizador* (o, sinónimamente, *excluidor*, *barra de Sheffer*, *barra de Nicod*, *conjuntor opuesto*, *negador alternativo* o *adjunción negada* [LORENZEN]), lo designamos por |; la incompatibilidad de p y q, por $p \mid q$, proposición que, como hemos dicho, es falsa sólo cuando ambas, p y q, son verdaderas.

Resumimos las condiciones de verdad de la incompatibilidad en la tabla de verdad

p	q	$p \mid q$
1	1	0
1	0	1
0	1	1
0	0	1

Observación 1.3.41.— También pudiésemos haber dicho que $p \mid q$ es una abreviatura de $\neg p \vee \neg q$, y utilizar las tablas de verdad del negador y de la disyunción, o bien una abreviatura de $\neg(p \wedge q)$, y utilizar las tablas de verdad del negador y de la conjunción.

[46] Cuidado porque en algunos textos se denomina *por negación alternativa*, lo que nos puede llevar a confusión por una posible connotación de exclusividad.

Ejemplo 84

Siendo:

$p_0 \fallingdotseq$ 6174 es un conjunto,

$q_0 \fallingdotseq$ 6174 es un número natural,

$p_{11} \fallingdotseq$ Ser 6174 un conjunto *es incompatible con* ser 6174 un número natural,

$Px \fallingdotseq x$ es una de mis amistades,

$Qx \fallingdotseq x$ dice siempre la verdad,

nos preguntamos:

0., ¿es verdadera la proposición representada por p_{11}?, y

1., ¿qué proposición representa $Px \mid Qx$?

Resolución.— Veamos:

- la proposición que representa p_{11} es verdadera porque es «p_0 es incompatible con q_0» y la proposición simple componente «6174 es un conjunto», en un sentido elemental, es falsa y la proposición simple componente «6174 es un número natural» es verdadera;
- $Px \mid Qx$ representa la proposición «que x sea una de mis amistades es incompatible con que x diga siempre la verdad».[47] ■

Para expresar la incompatibilidad de p y q, además de $p \mid q$, también se usan las designaciones $p \mathbin{\bar\wedge} q$, $p \not\wedge q$, $p \uparrow q$ y p/q.

Observación 1.3.42.— Es posible expresar la incompatibilidad $p \mid q$ como una disyunción de cubos y como una conjunción de cláusulas, en forma normal disyuntiva (FND) y en forma normal conjuntiva (FNC), respectivamente[48]. En efecto:

0. $\neg p \vee \neg q$, (FND)

1. $\neg p \vee \neg q$. (FNC)

Basta comprobar la igualdad de sus tablas de verdad para demostrarlo.

Observación 1.3.43.— Es posible expresar fácilmente $\neg p \vee \neg q$ como una conjunción, concretamente por $(\neg p \vee \neg q) \wedge \top$ (de nuevo, basta comprobar la igualdad de sus tablas de verdad para demostrar que es así).

[47] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).
[48] *Cfr. infra* § 3.1 (pág. 257 de esta edición).

Observación 1.3.44.— En el lenguaje ordinario también se usa la «o»; así, por ejemplo, en un contexto de haber presenciado una persona la no prestación de auxilio en un accidente, si dice «La furgoneta era una Boxer o una Jumpy», pudiese ser que no fuese ninguna de las dos, sino una Expert, o una Vito. La formulación dependerá de la seguridad de quien testifica, si la tiene, $p \veebar q$, si no la tiene, $p \mid q$.

Negación conjunta (negación de la disyunción)

Una proposición compuesta *por negación conjunta* (o, sinónimamente, *por disyunción opuesta*) es verdadera si, y sólo si, ambas proposiciones simples componentes son falsas. Por tanto, es falsa en los tres casos restantes.

En español, expresiones tales como, por ejemplo, las siguientes, expresan la *negación conjunta* de p y q, la prohibición de su disyunción.

- «ni p ni q»,
- «no p ni q».

El juntor correspondiente, llamado *negador conjunto* (o, sinónimamente, *flecha de Peirce*, *daga de Quine*, *inalternador* o *disyuntor opuesto*), lo designamos por $\downarrow$; la negación conjunta de p y q, por $p \downarrow q$, proposición que, como hemos dicho, es verdadera cuando ambas son falsas.

Resumimos las condiciones de verdad de la negación conjunta en la tabla de verdad

p	q	$p \downarrow q$
1	1	0
1	0	0
0	1	0
0	0	1

Observación 1.3.45.— También pudiésemos haber dicho que $p \downarrow q$ es una abreviatura de $\neg(p \vee q)$, y utilizar las tablas de verdad del negador y de la disyunción, o bien una abreviatura de $\neg\neg p \wedge \neg q$, y utilizar las tablas de verdad del negador y de la conjunción.

Ejemplo 85

Siendo:

$$p_0 \coloneqq \text{6174 es un conjunto},$$
$$q_0 \coloneqq \text{6174 es un número natural},$$
$$p_{12} \coloneqq \textit{Ni } \text{6174 es un conjunto } \textit{ni } \text{6174 es un número natural},$$
$$Px \coloneqq x \text{ es una de mis amistades},$$
$$Qx \coloneqq x \text{ dice siempre la verdad},$$

nos preguntamos:

0., ¿es verdadera la proposición representada por p_{12}?, y

1., ¿qué proposición representa $Px \downarrow Qx$?

Resolución.— Veamos:

- la proposición representada por p_{12} es falsa porque es «ni p_0 ni q_0» y la proposición simple componente «6174 es un conjunto», en un sentido elemental, es falsa y la proposición simple componente «6174 es un número natural» es verdadera, y
- $Px \downarrow Qx$ representa «ni x es una de mis amistades ni x dice siempre la verdad».[49] ■

Para expresar la negación conjunta de p y q, $p \downarrow q$, también se usan las designaciones $p \overline{\vee} q$, $p \forall q$ y $p \dagger q$.

Observación 1.3.46.— Es posible expresar la negación conjunta $p \downarrow q$ como una disyunción de cubos y como una conjunción de cláusulas, en forma normal disyuntiva (FND) y en forma normal conjuntiva (FNC), respectivamente[50]. En efecto:

0. $\neg p \wedge \neg q$; (FND)

1. $\neg p \wedge \neg q$. (FNC)

Basta comprobar la igualdad de sus tablas de verdad para demostrarlo.

Observación 1.3.47.— Es posible expresar fácilmente $\neg p \wedge \neg q$ como una disyunción, concretamente por $(\neg p \wedge \neg q) \vee \bot$ (de nuevo, basta comprobar la igualdad de sus tablas de verdad para demostrar que es así).

[49] *Cfr. supra* ejemplo 72 (pág. 77 de esta edición).
[50] *Cfr. infra* § 3.1 (pág. 257 de esta edición).

Observación 1.3.48.— Como estudiaremos en § 1.15 (pág. 161 de esta edición), en la base de juntores $\{\neg, \vee, \wedge\}$, insistamos en las reformulaciones que hemos destacado; por un lado, con el conjuntor como juntor principal,

- la contravalencia ($p \veebar q$): $(\neg p \vee \neg q) \wedge (p \vee q)$,
- la desimplicación ($p \nrightarrow q$): $p \wedge \neg q$,
- la desreplicación ($p \nleftarrow q$): $\neg p \wedge q$,
- la equivalencia ($p \leftrightarrow q$): $(\neg p \vee q) \wedge (p \vee \neg q)$,
- la negación conjunta ($p \downarrow q$): $\neg p \wedge \neg q$;

por otro, con el disyuntor como juntor principal,

- la contravalencia ($p \veebar q$): $(p \wedge \neg q) \vee (\neg p \wedge q)$,
- la implicación ($p \rightarrow q$): $\neg p \vee q$,
- la replicación($p \leftarrow q$): $p \vee \neg q$,
- la equivalencia ($p \leftrightarrow q$): $(p \wedge q) \vee (\neg p \wedge \neg q)$, y
- la incompatibilidad ($p \mid q$): $\neg p \vee \neg q$.

Nos encontraremos de nuevo con esta división cuando estudiemos los patrones y reglas de extensión en el subcapítulo dedicado a tablas semánticas[51].

Recordemos también la relación íntima entre la disyunción, la incompatibilidad y la contravalencia al expresar la alternación entre proposiciones:

- $p \vee q$ (disyunción): las alternativas p y q no se excluyen, aunque debe suceder una de ellas;
- $p \veebar q$ (contravalencia): las alternativas p y q se excluyen, aunque debe suceder una de ellas;
- $p \mid q$ (incompatibilidad): las alternativas p y q se excluyen, aunque puede no suceder ninguna de ellas.

[51] *Vid. infra* § 3.3 (pág. 274 de esta edición).

Ejemplo 86

Formalicemos:

0. Siempre que ha llovido ha escampado.
1. Mal me quieren mis comadres, porque les digo las verdades.
2. Bien me quieres, bien te quiero, mas no te doy mi dinero.
3. Agua que no has de beber, déjala correr.
4. Dolor no padecieres cuando, y sólo cuando, preverlo pudieres.
5. La mala gente no te estima o no te procura.
6. Canta la rana, y no tiene pelo ni lana.

[Cubit 4].

Resolución.—

0. $p \leftrightharpoons$ ha llovido; $q \leftrightharpoons$ ha escampado; $p \to q$ [implicación];
1. $p \leftrightharpoons$ mal me quieren mis comadres; $q \leftrightharpoons$ digo las verdades a mis comadres; $p \leftarrow q$ [replicación];
2. $p \leftrightharpoons$ me quieres bien; $q \leftrightharpoons$ te quiero bien; $r \leftrightharpoons$ te doy mi dinero; $(p \land q) \nrightarrow r$ [conjunción y desimplicación];
3. $p \leftrightharpoons$ puedes beber ese agua; $q \leftrightharpoons$ deja correr ese agua; $p \nleftarrow q$ [desreplicación];
4. $p \leftrightharpoons$ padeces dolor; $q \leftrightharpoons$ puedes prever el dolor; $\neg p \leftrightarrow q$ [negación y equivalencia];
5. $p \leftrightharpoons$ la mala gente te estima; $q \leftrightharpoons$ la mala gente te procura; $p \mid q$ [incompatibilidad];
6. $p \leftrightharpoons$ la rana canta; $q \leftrightharpoons$ la rana tiene pelo; $r \leftrightharpoons$ la rana tiene lana; $p \land (q \downarrow r)$ [conjunción y negación conjunta]. ■

Observación 1.3.49.— Pudiésemos practicar con más del refranero[52], de paso aprendiésemos por partida doble.

Observación 1.3.50.— A partir de una tabla de verdad podemos extraer relaciones interesantes. Por ejemplo, sea la tabla de verdad del implicador,

p	q	$p \to q$
1	1	1
1	0	0
0	1	1
0	0	1

Que las interpretaciones I_{11}, I_{01} y I_{00} sean modelos significa, respectivamente, que:

---

[52] *Vid. v. gr.* Sevilla y Zurdo [34].

- si p y q, entonces $p \to q$, esto es, $p \land q \to (p \to q)$;
- si no p y q, entonces $p \to q$, esto es, $\neg p \land q \to (p \to q)$, y
- si no p y no q, entonces $p \to q$, esto es, $\neg p \land \neg q \to (p \to q)$.

Que I_{10} sea un contramodelo significa que

- si p y no q, entonces no $p \to q$, esto es, $p \land \neg q \to \neg(p \to q)$.

Que conste, todo ha consistido en leer la tabla.

Finalicemos este apartado con otro ejemplo de formalización.

Ejemplo 87

Formalicemos (variables proposicionales y forma lógica):

0. Quien a hierro mata, a hierro muere.
1. Funcionará, siempre que lo hayas hecho bien.
2. En no queriendo, no hay pelea.
3. Sólo si estudias, aprenderás.
4. Aprenderás si estudias.
5. Aprenderás, a menos que hagas trampa.
6. Aprenderás, a menos que no estudies.
7. Esta IA es manipulable y, a igualdad de condiciones, más resoluta que aquélla.

[Cubit 5].

Resolución.— 0. Una forma lógica es $p \to q$, donde las variables proposicionales son: $p \leftrightharpoons$ Matar a hierro; $q \leftrightharpoons$ Morir a hierro. [Pensemos en su reescritura equivalente: Si se mata a hierro, entonces se muere a hierro].

1. Una forma lógica es $q \to p$, donde las variables proposicionales son: $p \leftrightharpoons$ Funcionar; $q \leftrightharpoons$ Hacerlo bien. [Pensemos en su reescritura equivalente: Si lo has hecho bien, entonces funcionará].

2. Una forma lógica es $\neg p \to \neg q$, donde las variables proposicionales son: $p \leftrightharpoons$ Querer pelea; $q \leftrightharpoons$ Haber pelea. [Pensemos en su reescritura equivalente: Si no se quiere (pelea), entonces no hay pelea].

3. Una forma lógica es $\neg q \to \neg p$, otra, $p \to q$, donde las variables proposicionales son: $p \leftrightharpoons$ Aprenderás; $q \leftrightharpoons$ Estudias. [Pensemos en sus reescrituras equivalentes: «Si no estudias, no aprenderás» o «Si has aprendido, entonces es que has estudiado»].

4. Una forma lógica es $q \to p$, donde las variables proposicionales son: $p \leftrightharpoons$ Aprenderás; $q \leftrightharpoons$ Estudias. [Pensemos en su reescritura equivalente: Si estudias, entonces aprenderás].

5. Una forma lógica es $\neg q \to p$, otra $p \lor q$, donde las variables proposicionales son: $p \leftrightharpoons$ Aprenderás; $q \leftrightharpoons$ Hagas trampa. [Pensemos en sus reescrituras equivalentes: «Si no haces trampa, entonces aprenderás» u «O aprendes o haces trampa» (ésta es disyunción y no contravalencia, pues pudiese suceder que aprendieses a pesar de hacer trampa)].

6. Una forma lógica es $q \to p$, otra $p \lor \neg q$, donde las variables proposicionales son: $p \leftrightharpoons$ Aprenderás; $q \leftrightharpoons$ Estudias. [Pensemos en sus reescrituras equivalentes: «Si estudias, entonces aprenderás» u «O aprendes o no estudias» (ésta es disyunción y no contravalencia, pues pudiese suceder que aprendieses a pesar de no estudiar)].

7. Una forma lógica es $p \land (q \to r)$, donde las variables proposicionales son: $p \leftrightharpoons$ Esta IA es manipulable; $q \leftrightharpoons$ Se da la igualdad de condiciones; $r \leftrightharpoons$ Esta IA es más resoluta que aquélla. [Pensemos en su reescritura equivalente: Esta IA es manipulable y si hay igualdad de condiciones, entonces es más resoluta que aquélla]. ■

§ 1.3.4 Composiciones de orden tres o superior

Nos preguntamos cómo expresar composiciones de orden tres o superior en la lógica de juntores. Estos juntores triádicos, tetrádicos, pentádicos, etc., corresponden a las funciones veritativas triádicas, tetrádicas, pentádicas, etc. Su número ya lo estudiamos en el teorema 1.3 (pág. 74 de esta edición).

Orden tres

Operador condicional

Un ejemplo de orden tres es el *operador condicional* `?:`, provisto en diversos lenguajes de programación, por ejemplo,

Datos: ϕ, ψ, χ
Resultado: ϕ ? ψ : χ
si ϕ **entonces**
  ψ;
en otro caso
  χ;
fin

Si bien en lógica de juntores no existe un signo para «`?:`», adoptaremos la notación «$\to,$», proveniente del lenguaje de programación combinado (en inglés, *Combined Programming Language*, o CPL), es decir, la expresión

$$\phi \mathbin{?} \psi : \chi$$

pudiésemos reescribirla en esta lógica de juntores «extendida» como

$$\phi \to \psi, \chi$$

a la que nos referiremos como *notación CPL del operador condicional* y la cual en lógica de juntores no es más que la conjunción de dos expresiones condicionales,

$$(\phi \to \psi) \wedge (\neg\phi \to \chi),$$

de significado

ϕ	ψ	χ	$(\phi$	$\to$	$\psi)$	$\boxed{\wedge}$	$(\neg$	ϕ	$\to$	$\chi)$
1	1	1	1	1	1	1	0	1	1	1
1	1	0	1	1	1	1	0	1	1	0
1	0	1	1	0	0	0	0	1	1	1
1	0	0	1	0	0	0	0	1	1	0
0	1	1	0	1	1	1	1	0	1	1
0	1	0	0	1	1	0	1	0	0	0
0	0	1	0	1	0	1	1	0	1	1
0	0	0	0	1	0	0	1	0	0	0

siendo *lógicamente equivalente* a

$$(\phi \wedge \psi) \vee (\neg\phi \wedge \chi)$$

(la equivalencia lógica de dos expresiones puede caracterizarse por tener la misma tabla de verdad y la designaremos con $\equiv$, así escribimos $(\phi \to \psi) \wedge (\neg\phi \to \chi) \equiv (\phi \wedge \psi) \vee (\neg\phi \wedge \chi)$; para saber más: *cfr. infra* § 1.13 [pág. 156 de esta edición]).

Recordemos que las letras griegas minúsculas «ϕ», «ψ», «χ», ... son metavariables que representan fórmulas cualesquiera.

Observación 1.3.51.— Se satisface, por ejemplo, que $\phi \wedge \psi$ es lógicamente equivalente a $\phi \to \psi, \phi$ y que $\phi \vee \psi$ es lógicamente equivalente a $\phi \to \phi, \psi$.

Observación 1.3.52.— Hemos usado la palabra operador, aún en el ámbito semántico e igualmente la usaremos en el sintáctico, por ahora en sentido ingenuo, esto es, en el mismo que usamos habitualmente los *operadores aritméticos* (por ejemplo, $+$, $-$, $\cdot$, $/$), los *operadores de comparación* (por ejemplo, $=$, $\neq$, $<$, $\leq$, $>$, $\geq$) o cualquier otro tipo de operadores que pudiésemos definir (por ejemplo, *operadores de comprobación* como el *operador de pertenencia* —designado por $\in (x, A)$, que es 1 precisamente si $x \in A$ y 0, en caso contrario— o el *operador de situación intermedia* —designado por $\between_{\preccurlyeq} (y, x, z)$, que es 1 precisamente si $x \preccurlyeq y \preccurlyeq z$ y 0, en caso contrario—). Más allá llegaremos tras estudiar el concepto de operación en un conjunto[53].

[53] *Cfr. infra* § 12.6 (pág. 701 de esta edición).

Observación 1.3.53.— La forma lógica $(\phi \wedge \psi) \vee (\neg\phi \wedge \chi)$, lógicamente equivalente a $(\phi \rightarrow \psi) \wedge (\neg\phi \rightarrow \chi)$, aparece, a veces, en la literatura, por ejemplo, en Wolfram|Alpha, con el nombre forma ITE[54]. Aunque son varias formas las lógicamente equivalentes al uso[55], en ciertas ocasiones, como ésta, puede que sea otra expresión lógicamente equivalente la que contribuya a aclarar lo afirmado. Por ejemplo, la propia afirmación

$$(p \wedge q) \vee (\neg p \wedge r),$$

parece que queda dicha de manera más clara en su expresión lógicamente equivalente

$$(p \rightarrow q) \wedge (\neg p \rightarrow r),$$

¿verdad?

Evaluación cortocircuitada

Existe una forma alternativa de evaluar la semántica de un juntor diádico, la *evaluación cortocircuitada*, la cual consiste en cumplir la norma de evaluar el segundo argumento sólo si el primero no basta para determinar el valor de la expresión dominada por el juntor en cuestión.

En el ámbito de la programación, los operadores cortocircuitados reciben nombres específicos, como `cand` (*and* condicional) y `cor` (*or* condicional) de Dijkstra[56], o designaciones específicas como && (para *cand*) y || (para *cor*) en lenguajes de programación concretos, estas últimas, por ejemplo, en C, Go, Java o Perl.

Las definiciones en lógica de juntores extendida con CPL, en función del operador condicional estudiado anteriormente, de `cand`, `cor` y `cimpl` (implicación cortocircuitada) son:

$$p \;\texttt{cand}\; q \leftrightharpoons p \rightarrow q, \bot;$$
$$p \;\texttt{cor}\; q \leftrightharpoons p \rightarrow \top, q;$$
$$p \;\texttt{cimpl}\; q \leftrightharpoons p \rightarrow q, \top;$$

es decir, la traducción a lógica de juntores es:

$$p \;\texttt{cand}\; q \longmapsto (p \rightarrow q) \wedge (\neg p \rightarrow \bot);$$
$$p \;\texttt{cor}\; q \longmapsto (p \rightarrow \top) \wedge (\neg p \rightarrow q);$$
$$p \;\texttt{cimpl}\; q \longmapsto (p \rightarrow q) \wedge (\neg p \rightarrow \top).$$

[54] *Cfr. infra* § 3.1.5 (pág. 269 de esta edición).
[55] *Cfr. infra* ejemplo 152 (pág. 270 de esta edición).
[56] *Cfr. v. gr.* Dijkstra [55] o Gries [56] (por cierto, dos libros que toda persona interesada en la programación de computadores debería estudiar de principio a fin).

Datos: p, q
Resultado: p `cand` q
si p **entonces**
  q;
en otro caso
  $\bot$;
fin

(a) p `cand` q

Datos: p, q
Resultado: p `cor` q
si p **entonces**
  $\top$;
en otro caso
  q;
fin

(b) p `cor` q

Datos: p, q
Resultado: p `cimpl` q
si p **entonces**
  q;
en otro caso
  $\top$;
fin

(c) p `cimpl` q

Figura 1.0.— Definiciones de `cand`, `cor` y `cimpl` en notación orientada a la programación.

Órdenes superiores

La *anidación de operadores condicionales* proporciona composiciones de órdenes superiores; por ejemplo,

Datos: $\phi, \psi, \rho, \sigma, \tau$
Resultado: $\phi\ ?\ \psi : (\rho\ ?\ \sigma : \tau)$
si ϕ **entonces**
  ψ;
en otro caso
  si ρ **entonces**
    σ;
  en otro caso
    τ;
  fin
fin

La expresión

$$\phi\ ?\ \psi : (\rho\ ?\ \sigma : \tau)$$

pudiésemos reescribirla en lógica de juntores extendida con la notación de CPL que hemos adoptado, como

$$\phi \to \psi, (\rho \to \sigma, \tau)$$

la cual en lógica de juntores no es más que la conjunción de tres expresiones condicionales,

$$(\phi \to \psi) \wedge (\neg\phi \wedge \rho \to \sigma) \wedge (\neg\phi \wedge \neg\rho \to \tau),$$

de significado

ϕ	ψ	ρ	σ	τ	$((\phi$	$\to$	$\psi)$	$\wedge$	$((\neg$	ϕ	$\wedge$	$\rho)$	$\to$	$\sigma))$	$\boxed{\wedge}$	$((\neg$	ϕ	$\wedge$	$\neg$	$\rho)$	$\to$	$\tau)$
1	1	1	1	1	1	1	1	1	0	1	0	1	1	1	1	0	1	0	0	1	1	1
1	1	1	1	0	1	1	1	1	0	1	0	1	1	1	1	0	1	0	0	1	1	0
1	1	1	0	1	1	1	1	1	0	1	0	1	1	0	1	0	1	0	0	1	1	1
1	1	1	0	0	1	1	1	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0
1	1	0	1	1	1	1	1	1	0	1	0	0	1	1	1	0	1	0	1	0	1	1
1	1	0	1	0	1	1	1	1	0	1	0	0	1	1	1	0	1	0	1	0	1	0
1	1	0	0	1	1	1	1	1	0	1	0	0	1	0	1	0	1	0	1	0	1	1
1	1	0	0	0	1	1	1	1	0	1	0	0	1	0	1	0	1	0	1	0	1	0
1	0	1	1	1	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1
1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0
1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	0	0	1	1	1
1	0	1	0	0	1	0	0	0	0	1	0	1	1	0	0	0	1	0	0	1	1	0
1	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	0	1	0	1	0	1	1
1	0	0	1	0	1	0	0	0	0	1	0	0	1	1	0	0	1	0	1	0	1	0
1	0	0	0	1	1	0	0	0	0	1	0	0	1	0	0	0	1	0	1	0	1	1
1	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0	0	1	0	1	0	1	0
0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	0	0	0	1	1	1
0	1	1	1	0	0	1	1	1	1	0	1	1	1	1	1	1	0	0	0	1	1	0
0	1	1	0	1	0	1	1	0	1	0	1	1	0	0	0	1	0	0	0	1	1	1
0	1	1	0	0	0	1	1	0	1	0	1	1	0	0	0	1	0	0	0	1	1	0
0	1	0	1	1	0	1	1	1	1	0	0	0	1	1	1	1	0	1	1	0	1	1
0	1	0	1	0	0	1	1	1	1	0	0	0	1	1	0	1	0	1	1	0	0	0
0	1	0	0	1	0	1	1	1	1	0	0	0	1	0	1	1	0	1	1	0	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	1	0	0	1	0	1	1	0	0	0
0	0	1	1	1	0	1	0	1	1	0	1	1	1	1	1	1	0	0	0	1	1	1
0	0	1	1	0	0	1	0	1	1	0	1	1	1	1	1	1	0	0	0	1	1	0
0	0	1	0	1	0	1	0	0	1	0	1	1	0	0	0	1	0	0	0	1	1	1
0	0	1	0	0	0	1	0	0	1	0	1	1	0	0	0	1	0	0	0	1	1	0
0	0	0	1	1	0	1	0	1	1	0	0	0	1	1	1	1	0	1	1	0	1	1
0	0	0	1	0	0	1	0	1	1	0	0	0	1	1	0	1	0	1	1	0	0	0
0	0	0	0	1	0	1	0	1	1	0	0	0	1	0	1	1	0	1	1	0	1	1
0	0	0	0	0	0	1	0	1	1	0	0	0	1	0	0	1	0	1	1	0	0	0

la cual es lógicamente equivalente a, por ejemplo, su forma ITE, de lectura más complicada:

$$(\rho \wedge ((\sigma \wedge ((\phi \wedge \psi) \vee (\neg\phi))) \vee ((\neg\sigma) \wedge \phi \wedge \psi))) \vee ((\neg\rho) \wedge ((\phi \wedge \psi) \vee ((\neg\phi) \wedge \tau))).$$

Otro ejemplo de *estructura alternativa múltiple* lo proporciona la instrucción `case`.

Datos: $\phi_0, \phi_1, \ldots, \phi_m$
Resultado: $x = a_0 \; ? \; \phi_0 \; : \; (x = a_1 \; ? \; \phi_1 \; : \ldots (x = a_m \; ? \; \phi_m) \ldots)$
seleccionar x **hacer**
  caso a_0 **hacer** ϕ_0;
  caso a_1 **hacer** ϕ_1;
  ⋮
  caso a_m **hacer** ϕ_m;
fin

La expresión

$$x = a_0 \; ? \; \phi_0 \; : \; (x = a_1 \; ? \; \phi_1 \; : \; (x = a_2 \; ? \; \phi_2 \; : \; (x = a_3 \; ? \ldots (x = a_m \; ? \; \phi_m) \ldots)))$$

pudiésemos reescribirla en lógica de juntores extendida con la igualdad y con la notación de CPL que hemos adoptado, como

$$x = a_0 \to \phi_0, (x = a_1 \to \phi_1, (x = a_2 \to \phi_2, (x = a_3 \to \ldots (x = a_m \to \phi_m) \ldots)))$$

la cual en lógica de juntores no es más que la conjunción de $m + 1$ expresiones condicionales,

$$((x = a_0) \to \phi_0) \wedge ((x = a_1) \to \phi_1) \wedge \ldots \wedge ((x = a_m) \to \phi_m).$$

§ 1.4 Número de interpretaciones de una fórmula

En el subcapítulo anterior hemos utilizado las tablas de verdad para representar las condiciones de verdad de proposiciones compuestas por un juntor con respecto a sus proposiciones simples componentes. Veamos aquí cuántas interpretaciones puede tener una fórmula, esto es, cuántas filas tiene su tabla de verdad.

Teorema 1.4
El número total de interpretaciones para una fórmula depende del número de sus variables proposicionales, siendo igual al número de filas de su tabla de verdad y correspondiendo cada fila a una única interpretación. De hecho, si en una fórmula ϕ intervienen n variables proposicionales, el número de interpretaciones para ϕ es 2^n.

Demostración.— Sea X un conjunto de n elementos. Cualquier aplicación del conjunto $\{1, 2, \ldots, k\}$ en X recibe el nombre de variación con repetición[57] de n elementos de X. Se demuestra que el número total de aplicaciones del conjunto $\{1, 2, \ldots, k\}$ en un conjunto de n elementos es $VR_n^k = n^k$. Para entender por qué el número de interpretaciones para una fórmula poliádica ϕ de

[57] *Vid. infra* definición 19.16 (pág. 1155 de esta edición).

n variables es 2^n, pensemos que una interpretación es una aplicación del conjunto $V_\phi(\subset \mathcal{V})$ de las n variables que aparecen en la fórmula ϕ en el conjunto $\{0, 1\}$, de dos elementos. ■

Ejemplo 88

Analicemos la afirmación «Que no venga ella y vengas tú es lo mismo que si no viniera él».

Resolución.— Siendo:

$p \leftrightharpoons$ viene ella,

$q \leftrightharpoons$ vienes tú,

$r \leftrightharpoons$ viene él.

entonces, la anterior afirmación se formaliza como

$$((no\ p)\ y\ q)\ es\ equivalente\ a\ (no\ r),$$

que en el lenguaje de la lógica de juntores se reescribe

$$(\neg p \wedge q) \leftrightarrow \neg r.$$

Como ya sabemos, como esta fórmula tiene tres variables de enunciado, existen para ella $2^3 = 8$ interpretaciones[58]:

$$\begin{aligned}
I_{000} &: \{p, q, r\} \to \{0, 1\}, \text{ definida por } I_{000}(p) = 0,\ I_{000}(q) = 0,\ I_{000}(r) = 0,\\
I_{001} &: \{p, q, r\} \to \{0, 1\}, \text{ definida por } I_{001}(p) = 0,\ I_{001}(q) = 0,\ I_{001}(r) = 1,\\
I_{010} &: \{p, q, r\} \to \{0, 1\}, \text{ definida por } I_{010}(p) = 0,\ I_{010}(q) = 1,\ I_{010}(r) = 0,\\
I_{011} &: \{p, q, r\} \to \{0, 1\}, \text{ definida por } I_{011}(p) = 0,\ I_{011}(q) = 1,\ I_{011}(r) = 1,\\
I_{100} &: \{p, q, r\} \to \{0, 1\}, \text{ definida por } I_{100}(p) = 1,\ I_{100}(q) = 0,\ I_{100}(r) = 0,\\
I_{101} &: \{p, q, r\} \to \{0, 1\}, \text{ definida por } I_{101}(p) = 1,\ I_{101}(q) = 0,\ I_{101}(r) = 1,\\
I_{110} &: \{p, q, r\} \to \{0, 1\}, \text{ definida por } I_{110}(p) = 1,\ I_{110}(q) = 1,\ I_{110}(r) = 0,\\
I_{111} &: \{p, q, r\} \to \{0, 1\}, \text{ definida por } I_{111}(p) = 1,\ I_{111}(q) = 1,\ I_{111}(r) = 1,
\end{aligned}$$

que quedan recogidas en las filas de la tabla de verdad asociada a dicha fórmula:

[58] *Cfr. supra* teorema 1.4 (pág. 116 de esta edición).

p	q	r	(*no* p	*y*	q)	*es equivalente a*	(*no* r)
			$\neg p$	$\land$	q	$\leftrightarrow$	$\neg r$
1	1	1	0	0	1	1	0
1	1	0	0	0	1	0	1
1	0	1	0	0	0	1	0
1	0	0	0	0	0	0	1
0	1	1	1	1	1	0	0
0	1	0	1	1	1	1	1
0	0	1	1	0	0	1	0
0	0	0	1	0	0	0	1

En definitiva, hay cuatro interpretaciones para las que la afirmación es verdadera y otras cuatro para las que no. Por ejemplo, la traducción directa de las interpretaciones para las que la afirmación es verdadera es:

I_{001}: Que no vengáis ni ella ni tú, pero sí venga él.

I_{010}: Que vengas tú, pero que no vengan ni ella ni él.

I_{101}: Que vengan ella y él y no vengas tú.

I_{111}: Que vengáis ella, él y tú.

Recordemos que decimos que estas cuatro interpretaciones I_{001}, I_{010}, I_{101} e I_{111} son modelos para la fórmula $(\neg p \land q) \leftrightarrow \neg r$ y que las otras cuatro interpretaciones son contramodelos para dicha fórmula. ■

§ 1.5 De la implicación directa e indirecta

Actividad 1.7

Aserto: Siempre es verdadera una implicación o su recíproca.

Justificación: Es posible demostrar que $(p \to q) \lor (q \to p)$ es verdadera; por ejemplo, si hacemos su tabla de verdad, observamos que todas las interpretaciones son modelos.

Contrajustificación: Sin embargo, si $p \leftrightharpoons n$ es impar y $q \leftrightharpoons n$ es primo, entonces $p \to q$ es falsa —por ejemplo, 9 es un impar no primo— y $q \to p$ es falsa —por ejemplo, 2 es un primo par—; en lenguaje llano, que no se satisface ninguna de las dos, así que no siempre es verdad la disyunción de una implicación y su recíproca.

Entonces, ¿en qué quedamos?, ¿es o no es verdadera?

Definición 1.10 (Implicación directa, recíproca, inversa y contrarrecíproca).— De una proposición en la forma $\phi \to \psi$ decimos que está en forma de implicación *directa*. Distinguimos tres formas asociadas:

- la *recíproca* de la proposición $\phi \to \psi$ es la proposición $\psi \to \phi$;
- la *inversa* (o, sinónimamente, *conversa*) de la proposición $\phi \to \psi$ es la proposición $\neg\phi \to \neg\psi$, y
- la *contrarrecíproca* (o, sinónimamente, *contrapositiva* o *coinversa*) de la proposición $\phi \to \psi$ es la proposición $\neg\psi \to \neg\phi$.

Teorema 1.5 (Algunas relaciones entre la forma directa y sus asociadas)

Se satisface:

0. $(\phi \to \psi) \leftrightarrow (\neg\psi \to \neg\phi)$, es decir, la directa y la contrarrecíproca son equivalentes, esto es, son ambas verdaderas o ambas falsas;
1. $(\psi \to \phi) \leftrightarrow (\neg\phi \to \neg\psi)$, es decir, la recíproca y la inversa son equivalentes, esto es, son ambas verdaderas o ambas falsas;
2. $(\phi \to \psi) \vee (\psi \to \phi)$, es decir, sucede la directa o su recíproca;
3. $(\phi \to \psi) \vee (\neg\phi \to \neg\psi)$, es decir, sucede la directa o su inversa;
4. $((\phi \to \psi) \to (\psi \to \phi)) \vee ((\psi \to \phi) \to (\phi \to \psi))$, es decir, la directa implica la recíproca o, recíprocamente, la recíproca implica la directa;
5. $((\phi \to \psi) \to (\neg\phi \to \neg\psi)) \vee ((\neg\phi \to \neg\psi) \to (\phi \to \psi))$, es decir, la directa implica la inversa o, recíprocamente, la inversa implica la directa;
6. $((\phi \to \psi) \to (\psi \to \phi)) \leftrightarrow ((\phi \to \psi) \to (\neg\phi \to \neg\psi))$, es decir, que la directa implique la recíproca es equivalente a que la directa implique la inversa.

Actividad 1.8

Demostremos el teorema 1.5 (pág. 119 de esta edición).

§ 1.6 Satisfactibilidad y validez

Definición 1.11.— Una fórmula ϕ es una *fórmula válida* (o, sinónimamente, *tautología* —cuidando de no confundirla con el juntor $\top$—) precisamente si es verdadera en todas sus interpretaciones, esto es, si, y sólo si, en su tabla de verdad figuran sólo unos, en otras palabras, cuando, y sólo cuando, toda interpretación para ϕ es un modelo para ϕ. Suele designarse por $\top$, aunque también son frecuentes en la literatura las designaciones 1, V y Υ (*verum*).

Definición 1.12.— Una fórmula ϕ es una *fórmula insatisfactible* (o, sinónimamente, *contradicción* —cuidando de no confundirla con el juntor $\bot$—) precisamente si es falsa en todas sus interpretaciones, esto es, si, y sólo si, en su tabla de verdad figuran únicamente ceros, en otras palabras, cuando,

y sólo cuando, ninguna interpretación para ϕ es un modelo para ϕ. Suele designarse por $\bot$, aunque también son frecuentes en la literatura las designaciones 0, F y $\curlywedge$ (*falsum*).

Observación 1.6.0.— La realidad de nuestra lengua natural es que en ella, una contradicción es cualquier proposición «lógicamente imposible», por ejemplo, «sucede P y, a la vez, no sucede P» (formalizada $p \wedge \neg p$). Esta observación tiene su razón de ser: ¿es verdadero o falso que «una niña de 10 años puede levantar una tonelada»? Si la niña no se ayuda de nada y está en condiciones de gravedad normal, parece imposible; pero ¿y si se ayuda de un sistema de palancas?, ¿o si está en condiciones de ingravidez?

Observación 1.6.1.— Si w es un modelo para una fórmula ϕ, pudiésemos también decir que ϕ es una *fórmula válida para la interpretación* w. Esta forma de hablar anticipa el concepto de *fórmula válida en un universo* U en lógica de cuantores.

Notemos que si para identificar las fórmulas válidas y fórmulas insatisfactibles utilizásemos los símbolos 1 y 0, éstos tendrían dos significados, a saber, por un lado, representan valores de verdad y por otro son fórmulas. Si adoptásemos los símbolos $\top$ y $\bot$, el alfabeto de $\mathcal{L}_0$ quedaría inmediatamente ampliado con ellos, en realidad con un conjunto de constantes $\{\top, \bot\}$.

Definición 1.13.— Una fórmula ϕ es una *fórmula contingente* (o, sinónimamente, *contingencia*, *indeterminación* o *fórmula anfótera*), precisamente si no es ni fórmula válida ni fórmula insatisfactible, es decir, si, y sólo si, en su tabla de verdad aparecen ceros y unos, en otras palabras, cuando, y sólo cuando, existen interpretaciones para ϕ que son modelos para ϕ y también existen interpretaciones para ϕ que no lo son.

Definición 1.14.— Una fórmula ϕ es una *fórmula satisfactible* (o, sinónimamente, *fórmula posible*), precisamente si es verdadera en alguna interpretación, esto es, si, y sólo si, en su tabla de verdad aparece algún uno, en otras palabras, cuando, y sólo cuando, alguna interpretación para ϕ es un modelo para ϕ.

Teorema 1.6
Toda fórmula contingente es satisfactible, mas no toda fórmula satisfactible es contingente.

Demostración.— La tautología es una fórmula satisfactible no contingente; de hecho es la única posible. ∎

Únicamente en los casos de fórmula insatisfactible y fórmula válida es posible hablar de valor de verdad de una proposición compuesta, el cual es 0 o 1, respectivamente. En el caso de ser contingencia se habla, a veces, de *valoración de verdad*.

Ejemplo 89

Proporcionemos un ejemplo de contingencia.

Resolución.— La tabla de verdad de la fórmula $p \wedge \neg q \leftrightarrow \neg r$ es

p	q	r	(p	$\wedge$	$\neg$	q)	$\boxed{\leftrightarrow}$	$\neg$	r
1	1	1	1	0	0	1	1	0	1
1	1	0	1	0	0	1	0	1	0
1	0	1	1	1	1	0	0	0	1
1	0	0	1	1	1	0	1	1	0
0	1	1	0	0	0	1	1	0	1
0	1	0	0	0	0	1	0	1	0
0	0	1	0	0	1	0	1	0	1
0	0	0	0	0	1	0	0	1	0

de la que deducimos que al existir modelos y contramodelos, dicha fórmula no es válida ni insatisfactible, pero sí contingente y, por lo tanto, satisfactible. ■

Observación 1.6.2.— El concepto de satisfactibilidad fue acuñado por Alfred TARSKI y tiene su origen en la matemática, en la que es costumbre usar expresiones del tipo «7 satisface la ecuación $x + 3 = 7$». En el ámbito de la lógica de juntores, a lo *satisfactible* también se le conoce como *consistente* y a lo *insatisfactible* como *inconsistente*. Esto se debe a que la lógica de juntores es correcta y completa, lo que hace que los conceptos de satisfactibilidad y consistencia coincidan[59].

Teorema 1.7

Si ϕ es una fórmula, entonces se satisface:

0. ϕ es válida si, y sólo si, $\neg\phi$ es insatisfactible;
1. ϕ es contingente si, y sólo si, $\neg\phi$ es contingente;
2. si ϕ es contingente, entonces ϕ es satisfactible.

Observación 1.6.3.— También se satisface lo siguiente.

3. Que ϕ sea satisfactible no implica que $\neg\phi$ sea insatisfactible (pensemos que la negación de una fórmula contingente también es una fórmula contingente).

Definición 1.15.— Decimos que Φ es un *conjunto satisfactible de fórmulas* precisamente si existe alguna interpretación que sea un modelo para Φ, en otras palabras, si, y sólo si, $\mathcal{M}(\Phi) \neq \emptyset$. En caso contrario decimos que es *insatisfactible*.

[59] *Vid. infra* teorema 6.9 (pág. 446 de esta edición).

Ejemplo 90

Demostremos que $\{p, \neg p\}$ es un conjunto insatisfactible de fórmulas.

Resolución.— En el ejemplo 67 (pág. 69 de esta edición) demostramos que no existe ningún modelo para dicho conjunto de fórmulas. ■

Ejemplo 91

Demostremos que $\{p \leftrightarrow q, \neg(\neg p \land q)\}$ es un conjunto satisfactible de fórmulas.

Resolución.— En el ejemplo 68 (pág. 70 de esta edición) demostramos que la interpretación I_{00} es un modelo para dicho conjunto de fórmulas. ■

Ejemplo 92

Demostremos que $\{p \land \neg q \leftrightarrow \neg r\}$ es un conjunto satisfactible de fórmulas.

Resolución.— En el ejemplo 89 (pág. 121 de esta edición) demostramos que las interpretaciones I_{111}, I_{100}, I_{011} e I_{001} son modelos para dicho conjunto de fórmulas. ■

Definición 1.16.— Decimos que Φ es un *conjunto finitamente satisfactible de fórmulas* precisamente si todos los subconjuntos finitos de fórmulas de Φ son satisfactibles.

Teorema 1.8
$\{\phi_0, \phi_1, \dots, \phi_n\}$ es un conjunto satisfactible de fórmulas si, y sólo si, $\phi_0 \land \phi_1 \land \cdots \land \phi_n$ es una fórmula satisfactible.

Si bien la posibilidad de que en la definición de conjunto satisfactible de fórmulas, dicho conjunto pudiese ser infinito, podría provocarnos cierta inquietud, el siguiente resultado se encarga de despejarla por completo.

Teorema 1.9 (Teorema de Compacidad)
Un conjunto de fórmulas es satisfactible si, y sólo si, es finitamente satisfactible.

Actividad 1.9

Demostremos que son satisfactibles:

0. $(p \to (q \land r)) \leftrightarrow ((p \to q) \land (p \to r))$ [$\to$ se distribuye por la izquierda en $\land$];
1. $(p \to (q \lor r)) \leftrightarrow ((p \to q) \lor (p \to r))$ [$\to$ se distribuye por la izquierda en $\lor$].

Actividad 1.10

Demostremos que son satisfactibles:

0. $((p \to r) \wedge (q \to r)) \to ((p \wedge q) \to r)$ [$\to$ se semidistribuye conversamente por la derecha en $\wedge$];
1. $((p \vee q) \to r) \to ((p \to r) \vee (q \to r))$ [$\to$ se semidistribuye por la derecha en $\vee$].

Actividad 1.11

Demostremos que son satisfactibles:

0. $((p \wedge q) \to r) \leftrightarrow ((p \to r) \vee (q \to r))$ [$\to$ se antidistribuye por la derecha en $\wedge$];
1. $((p \vee q) \to r) \leftrightarrow ((p \to r) \wedge (q \to r))$ [$\to$ se antidistribuye por la derecha en $\vee$].

El problema SAT

Saber si una fórmula de la lógica de juntores es satisfactible es uno de los problemas referentes en Complejidad Computacional, concretamente el problema SAT*, un problema NP-completo†. Es de interés, por tanto, el desarrollo de algoritmos de comprobación de la satisfactibilidad de un conjunto de fórmulas. El algoritmo DPLL/Davis-Putnam-Logemann-Loveland‡ y WalkSAT§ son de uso popular.

* *Vid. v. gr.* https://es.wikipedia.org/wiki/Problema_de_satisfacibilidad_booleana.
† *Vid. v. gr.* https://es.wikipedia.org/wiki/NP-completo.
‡ *Vid. v. gr.* https://es.wikipedia.org/wiki/Algoritmo_DPLL.
§ *Vid. v. gr.* https://en.wikipedia.org/wiki/WalkSAT.

§ 1.7 Redefinición de interpretación

Definición 1.17 (Redefinición de interpretación).— Formalmente, lo que hemos hecho es construir, guiados por la semántica de nuestra lógica ordinaria, una *extensión de la definición de interpretación*[60], del conjunto de todas las variables proposicionales $\mathcal{V}$ al conjunto de todas las fórmulas $\mathcal{F}_0$, $I : \mathcal{F}_0 \longrightarrow \{0, 1\}$, sujeta a las condiciones siguientes (extensión, que abusando del lenguaje, seguiremos notando por I y llamando interpretación); siendo ϕ y ψ fórmulas,

0. $I(\neg\phi) = 1$ si, y sólo si, $I(\phi) = 0$,
1. $I(\phi \wedge \psi) = 1$ si, y sólo si, $I(\phi) = 1$ y $I(\psi) = 1$,
2. $I(\phi \veebar \psi) = 0$ si, y sólo si, $I(\phi) = I(\psi)$,
3. $I(\phi \vee \psi) = 1$ si, y sólo si, $I(\phi) = 1$ o $I(\psi) = 1$,
4. $I(\phi \to \psi) = 0$ si, y sólo si, $I(\phi) = 1$ y $I(\psi) = 0$,
5. $I(\phi \leftrightarrow \psi) = 1$ si, y sólo si, $I(\phi) = I(\psi)$,

[60] *Cfr. supra* definición 1.1 (pág. 64 de esta edición).

6. $I(\phi \mid \psi) = 0$ si, y sólo si, $I(\phi) = 1$ y $I(\psi) = 1$,

7. $I(\phi \downarrow \psi) = 1$ si, y sólo si, $I(\phi) = 0$ y $I(\psi) = 0$.

§ 1.8 Satisfactibilidad y tablas de verdad: más ejemplos

Insistamos en que las tablas de verdad permiten analizar la satisfactibilidad de una fórmula, esto es, determinar si es insatisfactible, contingente o válida[61].

. . . .

Para las siguientes cuestiones, hagamos esto, cuando sea posible.

0. Hallemos el argumento equivalente a la argumentación dada. Llamemos a aquél, $\mathcal{A}$.
   - Reescribamos la argumentación. (Optativo).
   - Escribamos el argumento ($\mathcal{A}$).
   - Exploremos intuitivamente su validez. (Optativo).
1. Formalicemos dicho argumento en lógica de juntores.
   - Nombremos las variables proposicionales que representan las proposiciones simples.
   - Analicemos su estructura lógico-gramatical. (Optativo).
   - Proporcionemos su esquema argumental.
   - Hallemos su forma lógica.
2. Demostremos si $\mathcal{A}$ es o no es un argumento válido. Utilicemos las tablas de verdad, como *estrategia de verificación* —esto es, intentamos demostrar que todas las interpretaciones son modelos para la fórmula correspondiente a $\mathcal{A}$— y como *estrategia de refutación* —esto es, intentamos refutar que exista un contramodelo para la fórmula correspondiente a $\mathcal{A}$, para lo que trabajamos «hacia atrás», suponemos no $\mathcal{A}$ y vamos eliminando todas las interpretaciones que no puedan ser un contramodelo de $\mathcal{A}$—.
   I. Resolución de $\mathcal{A}$ utilizando las tablas de verdad como estrategia de verificación.
   II. Identifiquemos el conjunto decisor para $\mathcal{A}$, esto es, el conjunto Γ de fórmulas bien formadas tal que los modelos para Γ son los contramodelos para $\mathcal{A}$.

[61] Más o menos fue sobre 1880 cuando se inició esta pauta de razonamiento según las tablas de verdad; se debe, principalmente, a FREGE, PEIRCE y SCHRÖDER. Sus grandes divulgadores son RUSSELL y WITTGENSTEIN, sobre 1920. La forma más compacta de hacerlo, que ilustra el ejemplo 93 (pág. 125 de esta edición) es de QUINE [57].

iii. Resolución de $\mathcal{A}$ utilizando las tablas de verdad como estrategia de refutación: estudiemos si existe una refutación para Γ —esto es, si encontramos que la tabla para Γ es una tabla insatisfactible—, una tabla de refutación, para Γ.

3.
- Si $\mathcal{A}$ resultó ser un argumento válido, finalicemos o, alternativa, mas sólo optativamente, modifiquemos las premisas o la conclusión para que el argumento modificado no sea válido, justifiquemos su no validez y continuemos.
- Si $\mathcal{A}$ no es válido, identifiquemos los modelos para Γ que proporciona la tabla para Γ.

4. Caso de que existan modelos para Γ, utilicemos las tablas de verdad como estrategia de verificación para demostrar que dichos modelos lo son para Γ.

5. Si existen modelos para Γ, expresemos en español las contraargumentaciones, construidas a partir de dichos modelos, que permiten refutar la argumentación dada (optativamente, también presentaremos los contraargumentos para $\mathcal{A}$).

Ejemplo 93

¿Es válida la siguiente argumentación condicional: «Si el programa de cooperación en la sostenibilidad para el desarrollo (PCSD) no se frustra, entonces el PCSD debe comenzar y terminar. El PCSD comenzó y se frustró. Por lo tanto, el PCSD no terminó.»?

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si el PCSD no se frustra, entonces el PCSD comienza y el PCSD termina. El PCSD comienza y el PCSD se frustra. Luego, el PCSD no termina.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.
   - *Variables proposicionales*.

     Siendo el universo de discurso la colección de todas las iniciativas económicas, políticas y sociales, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

$$f \coloneqq \text{el PCSD se frustra,}$$
$$c \coloneqq \text{el PCSD comienza,}$$
$$t \coloneqq \text{el PCSD termina.}$$

- *Esquema argumental*:

  Si se supone no f, se sigue c y t.
  Se tiene c y f.
  ___
  $\therefore$ Se sigue no t.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{\neg f \to c \wedge t, c \wedge f\}$ y la conclusión ψ, a saber, $\neg t$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(\neg f \to c \wedge t) \wedge (c \wedge f) \to \neg t$. Llamémosla A.

2. *Demostración de si $\mathcal{A}$ es o no es un argumento válido*.

   I. *Resolución de $\mathcal{A}$ utilizando tablas de verdad como estrategia de verificación*.

   Por ejemplo, con una tabla de verdad utilizada como estrategia de verificación de A.

c	f	t	$((\neg$	f	$\to$	$(c$	$\wedge$	$t))$	$\wedge$	$(c$	$\wedge$	$f))$	$\boxed{\to}$	$\neg$	t
1	1	1	0	1	1	1	1	1	1	1	1	1	0	0	1
1	1	0	0	1	1	1	0	0	1	1	1	1	1	1	0
1	0	1	1	0	1	1	1	1	0	1	0	0	1	0	1
1	0	0	1	0	0	1	0	0	0	1	0	0	1	1	0
0	1	1	0	1	1	0	0	1	0	0	0	1	1	0	1
0	1	0	0	1	1	0	0	0	0	0	0	1	1	1	0
0	0	1	1	0	0	0	0	1	0	0	0	0	1	0	1
0	0	0	1	0	0	0	0	0	0	0	0	0	1	1	0

   Al existir un contramodelo para A, ésta es una fórmula no válida, de donde $\mathcal{A}$ es un argumento no válido e, igualmente, la argumentación es no válida.

   II. *Identificación del conjunto Γ*.

   Identificamos la estructura de $\mathcal{A}$ con ser $\phi_0 \wedge \phi_1 \to \psi$ una fórmula válida. Por el teorema 1.2 (pág. 71 de esta edición) sabemos que w es un contramodelo para dicha fórmula si, y sólo si, w es un modelo para Γ, donde $\Gamma = \Phi \cup \{\neg\psi\} = \{\neg f \to c \wedge t, c \wedge f, t\}$.

   III. *Resolución de $\mathcal{A}$ utilizando las tablas de verdad como estrategia de refutación*.

   Estudiemos si existe una refutación para Γ —esto es, si utilizando la tabla de verdad como estrategia de refutación encontramos que la tabla para Γ es una tabla insatisfactible—, una tabla de refutación, para Γ.

   Tenemos dos posibilidades de estudio equivalentes:

   A. estudiar la tabla para Γ, partiendo de su verdad: que busquemos modelos para las tres significa que deben serlo para cada una, en particular, t es verdadera y $c \wedge f$ es verda-

dera y de ésta, por ser una conjunción, tenemos que c y f son verdaderas; en definitiva, sólo hemos de considerar la interpretación I_{111},

$c\ f\ t$	$\neg\ f \rightarrow (\ c\ \wedge\ t\ )$	$c\ \wedge\ f$	t
1 1 1	0 1 $\boxed{1}$ 1 1 1	1 $\boxed{1}$ 1	$\boxed{1}$

lo que traducido al lenguaje de la lógica de juntores, equivale a estudiar la tabla para $(\neg f \rightarrow c \wedge t) \wedge (c \wedge f) \wedge t$, partiendo de su verdad: que la conjunción sea verdadera lleva a que cada conjunto lo es, en particular, t es verdadero y $c \wedge f$ es verdadero y de ésta, análogamente, por ser una conjunción, tenemos que c y f son verdaderas; en definitiva, sólo hemos de considerar la interpretación I_{111},

$c\ f\ t$	$((\neg\ f\ \rightarrow\ c\ \wedge\ t\ ) \wedge (\ c\ \wedge\ f\ ))\ \wedge\ t$
1 1 1	0 1 1 1 1 1 1 1 1 1 $\boxed{1}$ 1

o bien,

B. alternativamente, estudiar la tabla para la fórmula $(\neg f \rightarrow c \wedge t) \wedge (c \wedge f) \rightarrow \neg t$, partiendo de su falsedad, puesto que se satisface que[62] w es un modelo para $(\phi_0 \wedge \phi_1) \wedge \psi$ si, y sólo si, w es un contramodelo para $(\phi_0 \wedge \phi_1) \wedge \neg\psi$: nuestro punto de comienzo es la negación de la implicación, esto es, $\neg t$ es falsa, es decir, t es verdadera, y$(\neg f \rightarrow c \wedge t) \wedge (c \wedge f)$ verdadera y de ser la segunda una conjunción y tener que ser verdad, sabemos que $[\![c]\!] = 1$ y también $[\![f]\!] = 1$; en otras palabras, sólo hemos de considerar la interpretación I_{111},

$c\ f\ t$	$((\neg\ f\ \rightarrow (\ c\ \wedge\ t\ )) \wedge (\ c\ \wedge\ f\ )) \rightarrow\ \neg\ t$
1 1 1	0 1 1 1 1 1 1 1 1 1 $\boxed{0}$ 0 1

en otras palabras, existe un modelo para Γ, o lo que es equivalente, un contramodelo para $\mathcal{A}$, por lo que $\mathcal{A}$ es un argumento no válido y, en definitiva, la argumentación es no válida.

3. *Identificación de los modelos para Γ que proporciona la tabla para Γ.*

   En dicha tabla para Γ apreciamos que la interpretación I_{111} es un contramodelo para A y por tanto un modelo para Γ.

4. *Demostración de que los modelos lo son para Γ.*

   La tabla de 2.III.A. demuestra que I_{111} es un modelo para Γ.

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

   Una contraargumentación construida a partir de I_{111} es la siguiente.

   Caso que el PCSD se frustre, comience y termine, se satisface la primera premisa (es un condicional con antecedente falso, ya que no es cierto que el PCSD no se frustre, pues se frustra) y

[62] *Cfr. supra* teorema 1.2 (pág. 71 de esta edición).

también se satisface la segunda premisa (el PCSD comienza y se frustra), pero no se satisface la conclusión (es falso que el PCSD no termine, pues termina). ■

Ejemplo 94

Nos informan de que si Sara no quiere, Wanda quiere. Y de que es imposible que los asertos «Sara quiere» y «Camila no puede» se satisfagan a la vez. Además, nos aseguran que si Wanda quiere, entonces Sara quiere y Camila puede. ¿Es válido concluir que Camila puede?

[Cubit 9], [SEL 1:2], *Cfr.* SDC [58]: 4. *Some Computer Problems*, § 3 *A Problem Involving Three Girls* (págs. 57–60).

Resolución.—

0. *Argumento* ($\mathcal{A}$) (concluyendo que Camila puede): Si Sara no quiere, entonces Wanda quiere. Es falso que simultáneamente Sara quiera y Camila no pueda. Si Wanda quiere, entonces Sara quiere y Camila puede. Luego, Camila puede.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales.*

     Siendo el universo de discurso el conjunto de todas las personas, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

     $$s \leftrightharpoons \text{Sara quiere,}$$
     $$w \leftrightharpoons \text{Wanda quiere,}$$
     $$c \leftrightharpoons \text{Camila puede.}$$

   - *Esquema argumental* (concluyendo que Camila puede):

     Si se supone no s, se sigue w.
     Se tiene que no suceden a la vez s y no c.
     Si se supone w, se sigue s y c.
     ___
     ∴ Se sigue c.

   - *Forma lógica.*

     Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2\} = \{\neg s \to w, \neg(s \wedge \neg c), w \to (s \wedge c)\}$ y la conclusión ψ, a saber, c. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(\neg s \to w) \wedge \neg(s \wedge \neg c) \wedge (w \to (s \wedge c)) \to c$. Llamémosla A.

2. *Demostración de si $\mathcal{A}$ es o no es un argumento válido.*

I. *Resolución de $\mathcal{A}$ utilizando tablas de verdad como estrategia de verificación.*

Por ejemplo, con una tabla de verdad utilizada como estrategia de verificación de A.

c	s	w	$(((\neg$	s	$\to$	$w)$	$\wedge$	$\neg($	s	$\wedge$	$\neg$	$c))$	$\wedge$	$(w$	$\to$	$(s$	$\wedge$	$c)))$	$\boxed{\to}$	c
1	1	1	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1
1	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	1	1	1	1
1	0	1	1	0	1	1	1	1	0	0	0	1	0	1	0	0	0	1	1	1
1	0	0	1	0	0	0	0	1	0	0	0	1	0	0	1	0	0	1	1	1
0	1	1	0	1	1	1	0	0	1	1	1	0	0	1	0	1	0	0	1	0
0	1	0	0	1	1	0	0	0	1	1	1	0	0	0	1	1	0	0	1	0
0	0	1	1	0	1	1	1	1	0	0	1	0	0	1	0	0	0	0	1	0
0	0	0	1	0	0	0	0	1	0	0	1	0	0	0	1	0	0	0	1	0

En ella apreciamos que todas las interpretaciones son modelos, por lo que A es una fórmula válida. Por lo tanto, $\mathcal{A}$ es un argumento válido, al igual que es válida la argumentación «Se sabe que si Sara no quiere, Wanda quiere; que es imposible que los asertos "Sara quiere" y "Camila no puede" se satisfagan a la vez, y que si Wanda quiere, entonces Sara quiere y Camila puede. De esta información se concluye que Camila puede».

II. *Identificación del conjunto* Γ.

Identificamos la estructura de $\mathcal{A}$ con ser $\phi_0 \wedge \phi_1 \wedge \phi_2 \to \psi$ una fórmula válida. Por el teorema 1.2 (pág. 71 de esta edición) sabemos que w es un contramodelo para dicha fórmula si, y sólo si, w es un modelo para Γ, donde $\Gamma = \Phi \cup \{\neg\psi\} = \{\neg s \to w, \neg(s \wedge \neg c), w \to (s \wedge c), \neg c\}$.

III. *Resolución de $\mathcal{A}$ utilizando las tablas de verdad como estrategia de refutación.*

En lógica de juntores, $(\phi \to \bot) \leftrightarrow \neg\phi$ es una fórmula válida, cuya implicación $(\phi \to \bot) \to \neg\phi$ nos interesa en este momento como esencia del método de *demostración por reducción al absurdo* (RAA) (o, sinónimamente, *por contradicción*), que aplicamos aquí en anticipación: si de suponer que sucede ϕ se sigue una fórmula insatisfactible, entonces no sucede ϕ.

Ser modelo para Γ se traduce en lógica de juntores en ser modelo para $(\neg s \to w) \wedge \neg(s \wedge \neg c) \wedge (w \to (s \wedge c)) \wedge \neg c$.

Sea $\phi \leftrightharpoons$ existe un modelo para $(\neg s \to w) \wedge \neg(s \wedge \neg c) \wedge (w \to (s \wedge c)) \wedge \neg c$. Demostremos que suponer ϕ conduce a una fórmula insatisfactible, por lo que por RAA habríamos demostrado que lo que se satisface es $\neg\phi$.

Analicemos $(\neg s \to w) \wedge \neg(s \wedge \neg c) \wedge (w \to (s \wedge c)) \wedge \neg c$: si existiese un modelo para ella, por ser una conjunción, todos los conjuntos serían verdad, en particular, $\neg s \to w$ es verdadera (*); y también $\neg c$, de donde $[\![c]\!] = 0$; de la verdad de $\neg c$ y de la de $\neg(s \wedge \neg c)$, se sigue

$[\![s]\!] = 0$; por lo tanto, $s \wedge c$ es falsa y como $w \to (s \wedge c)$ es verdadera, obliga a ser $[\![w]\!] = 0$; por ser $[\![s]\!] = 0$ y $[\![w]\!] = 0$, se sigue que $\neg s \to w$ es falsa (†); he aquí lo insatisfactible, la contradicción, por (*) y (†), tenemos a la vez que $\neg s \to w$ es verdadera y falsa. Como $\phi \to \bot$, esto es, suponer que existe un modelo para $(\neg s \to w) \wedge \neg(s \wedge \neg c) \wedge (w \to (s \wedge c)) \wedge \neg c$ conduce a una fórmula insatisfactible, entonces, de RAA, se sigue $\neg\phi$, es decir, que no existe ningún modelo para dicha fórmula, o sea, no existe ningún modelo para Γ, o lo que es equivalente, ningún contramodelo para $\mathcal{A}$ por lo que $\mathcal{A}$ es un argumento válido y, en definitiva, la argumentación es válida.

3. No procede (la argumentación es válida).

4. No procede (la argumentación es válida).

5. No procede (la argumentación es válida). ■

Observación 1.8.0.— Hemos hecho los apartados 2.II y 2.III por motivos pedagógicos; caso de que, como en este ejemplo, en 2.I demostremos la validez de $\mathcal{A}$ no es necesario desarrollar 2.II y 2.III (aunque seguro que es una buena idea hacerlo optativamente, para practicar RAA).

Ejemplo 95

Tras diversas consultas sesudas, el ministerio correspondiente publicó un comunicado de prensa en el que razonaron así: «Una manera de lograr que la contaminación sea aceptable es conseguir que circulen menos automóviles por las carreteras. Una manera de que circulen menos automóviles es cobrar por usar las carreteras. Si circulan menos coches por las carreteras, la temperatura atmosférica del país descenderá. Esta primavera ha hecho más frío. La conclusión es ineludible: la contaminación es aceptable». ¿Es válida esta argumentación?

[Cubit 13], [EFO 24.5.2018:1], [EFO 20.5.2022:1] (argumento $\mathcal{A}$), [SEL 1:3] (argumento $\mathcal{A}$). *Cfr.* Crilly [59]: capítulo 16: Lógica (págs. 72–73).

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si hay menos coches en las carreteras, entonces la contaminación será aceptable. Si hay que pagar por usar las carreteras, entonces habrá menos coches en las carreteras. Si hay menos coches en las carreteras, entonces la temperatura atmosférica descenderá. La temperatura atmosférica ha descendido. Luego, la contaminación es aceptable.

   (Que la primavera sea más fría simplemente corrobora que la temperatura desciende y recíprocamente).

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

- *Variables proposicionales*.

  Siendo el universo de discurso la realidad pasada, presente y futura del territorio en cuestión, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

  $c \fallingdotseq$ Hay menos coches en las carreteras;

  $p \fallingdotseq$ La contaminación será aceptable;

  $s \fallingdotseq$ Hay que pagar por usar las carreteras;

  $d \fallingdotseq$ La temperatura atmosférica descenderá.

- *Esquema argumental*:

  Si se supone c, se sigue p.
  Si se supone s, se sigue c.
  Si se supone c, se sigue d.
  Se tiene d.
  $\therefore$ Se sigue p.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2, \phi_3\} = \{c \to p, s \to c, c \to d, d\}$ y la conclusión ψ, a saber, p. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(c \to p) \land (s \to c) \land (c \to d) \land d \to p$. Llamémosla A.

2. *Demostración de si $\mathcal{A}$ es o no es un argumento válido*.

   1. *Resolución de $\mathcal{A}$ utilizando tablas de verdad como estrategia de verificación*.

      Demostremos que el argumento A no es lógicamente válido. Para ello, utilicemos las tablas de verdad como estrategia de verificación.

c	d	p	s	$((((c$	$\to$	$p)$	$\wedge$	$(s$	$\to$	$c))$	$\wedge$	$(c$	$\to$	$d))$	$\wedge$	$d)$	**$\to$**	p
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
1	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1
1	1	0	1	1	0	0	0	1	1	1	0	1	1	1	0	1	1	0
1	1	0	0	1	0	0	0	0	1	1	0	1	1	1	0	1	1	0
1	0	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	1	1
1	0	1	0	1	1	1	1	0	1	1	0	1	0	0	0	0	1	1
1	0	0	1	1	0	0	0	1	1	1	0	1	0	0	0	0	1	0
1	0	0	0	1	0	0	0	0	1	1	0	1	0	0	0	0	1	0
0	1	1	1	0	1	1	0	1	0	0	0	0	1	1	0	1	1	1
0	1	1	0	0	1	1	1	0	1	0	1	0	1	1	1	1	1	1
0	1	0	1	0	1	0	0	1	0	0	0	0	1	1	0	1	1	0
0	1	0	0	0	1	0	1	0	1	0	1	0	1	1	1	1	0	0
0	0	1	1	0	1	1	0	1	0	0	0	0	1	0	0	0	1	1
0	0	1	0	0	1	1	1	0	1	0	1	0	1	0	0	0	1	1
0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	0	0	1	0
0	0	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0

En esta tabla apreciamos que en la columna del juntor principal, no todos los valores son 1; por lo tanto, A no es una fórmula válida, de donde $\mathcal{A}$ no es un argumento lógicamente válido e, igualmente, la argumentación no es válida.

II. *Identificación del conjunto* Γ.

Identificamos la estructura de $\mathcal{A}$ con ser $\phi_0 \wedge \phi_1 \wedge \phi_2 \wedge \phi_3 \to \psi$ una fórmula válida. Por el teorema 1.2 (pág. 71 de esta edición) sabemos que w es un contramodelo para dicha fórmula si, y sólo si, w es un modelo para Γ, donde $\Gamma = \Phi \cup \{\neg\psi\} = \{c \to p, s \to c, c \to d, d, \neg p\}$.

III. *Resolución de* $\mathcal{A}$ *utilizando las tablas de verdad como estrategia de refutación*.

Estudiemos si existe una refutación para Γ —esto es, si utilizando la tabla de verdad como estrategia de refutación encontramos que la tabla para Γ es una tabla insatisfactible—, una tabla de refutación, para Γ.

Como vimos en el apartado 2.III del ejemplo 93 (pág. 125 de esta edición), debido al teorema 1.2 (pág. 71 de esta edición), es posible estudiar la tabla para Γ, esto es, la tabla para $(c \to p) \wedge (s \to c) \wedge (c \to d) \wedge d \wedge \neg p$, a partir de su verdad (*cfr.* 2.III.A de dicho ejemplo) —encontrando un modelo para Γ (o lo que es equivalente, un contramodelo para $\mathcal{A}$)— o, equivalentemente, la tabla para $(c \to p) \wedge (s \to c) \wedge (c \to d) \wedge d \to p$, a partir de su falsedad (*cfr.* 2.III.B de dicho ejemplo).

Estudiamos esta última en el caso presente. Nuestro punto de comienzo es la falsedad de $(c \to p) \land (s \to c) \land (c \to d) \land d \to p$, esto es, su negación, $\neg((c \to p) \land (s \to c) \land (c \to d) \land d \to p)$, que por ser ésta equivalente a $(c \to p) \land (s \to c) \land (c \to d) \land d \land \neg p)$, supone la negación de la conclusión —es decir, que $\neg p$ es verdadera—, esto es, que p es falsa, y como nuestro objetivo es encontrar un modelo para las cuatro hipótesis, en particular, de la sencillez de la cuarta hipótesis (es un literal) sabemos que d es verdadera. Esta interpretación —$[\![d]\!] = 1$, $[\![p]\!] = 0$— reduce la tabla de verdad de $(c \to p) \land (s \to c) \land (c \to d) \land d \to p$ a cuatro filas, si bien, como podremos apreciar en la discusión que sigue, en realidad sólo será necesario razonar con dos de ellas:

c	s	((((c	$\to$	$\bot$)	$\land$ (	s	$\to$	c))	$\land$ (	c	$\to$	$\top$))	$\land$	$\top$)	$\to$	$\bot$
1	1	1	0	0	0	1	1	1	0	1	1	1	0	1	1	0
1	0	1	0	0	0	0	1	1	0	1	1	1	0	1	1	0
0	1	$\boxed{0}$	$\boxed{1}$	$\boxed{0}$	0	1	0	$\boxed{0}$	0	0	1	1	0	1	1	0
0	0	$\boxed{0}$	$\boxed{1}$	$\boxed{0}$	1	$\boxed{0}$	$\boxed{1}$	$\boxed{0}$	1	0	1	1	1	1	0	0

Un recorrido por los siguientes pasos en la tabla: de ser verdadera $c \to \bot$, deducimos que c es falsa, y por la misma razón, ahora de la verdad de $s \to c$, s es falsa.

De hecho, siguiendo esta explicación, pudiésemos haber trabajado sólo con la interpretación I_{0100} (por tratarse de subfórmulas sencillas, pues, en general, con subfórmulas complejas, hacerlo sin tabla hubiese sido harto complicado).

En definitiva, utilizando la tabla de verdad como estrategia de refutación hemos encontrado un contramodelo para $\mathcal{A}$ —o lo que es equivalente, un modelo para Γ—, por lo que $\mathcal{A}$ no es un argumento válido y, en definitiva, la argumentación es no válida.

3. *Identificación de los modelos para* Γ *que proporciona la tabla para* Γ.

   Vía las tablas de verdad, tanto como estrategia de verificación como de refutación, concluimos que la interpretación I_{0100} es el único modelo para Γ (por ser el único contramodelo para A).

4. *Demostración de que los modelos lo son para* Γ.

   Demostremos que I_{0100} es un modelo para Γ; para ello, estudiemos la valoración de verdad de las fórmulas de Γ con dicha interpretación:

c	d	p	s	c	$\to$	p	s	$\to$	c	c	$\to$	d	d	$\neg$	p
0	1	0	0	0	$\boxed{1}$	0	0	$\boxed{1}$	0	0	$\boxed{1}$	1	$\boxed{1}$	$\boxed{1}$	0

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos*.

   Una contraargumentación en español construida a partir de I_{0100} pudiese ser la siguiente (recordemos que la lógica de juntores no es una lógica temporal).

Cuando no hay menos coches en las carreteras y la contaminación no es aceptable y no hay que pagar por usar las carreteras y la temperatura atmosférica desciende, se satisfacen las cuatro premisas, pero no la conclusión, pues ésta afirma que la contaminación es aceptable. ■

Observación 1.8.1.— Para la resolución de estas cuestiones, pudiésemos apoyarnos en alguno de los artefactos existentes en línea. Por ejemplo, Truth Table Generator[63] o Logic Calculator[64] —en éste existen signos para la fórmula válida (W) y la fórmula insatisfactible (F), a diferencia de aquél en el que sólo existe para la insatisfactible (#)—. Asimismo pudiésemos haber escrito un programa en algún lenguaje de programación conveniente o favorito, como Sage[65] u otros[66].

Ejemplo 96

Recordemos el ejemplo 95 (pág. 130 de esta edición). Pues bien, resulta que sucedió que un medio de comunicación publicó lo que dijo el ministerio así: «Si hay menos automóviles en las carreteras, la contaminación será aceptable. O bien tenemos menos automóviles en las carreteras, o bien se tendría que cobrar por el uso de las carreteras, o bien ambas cosas. Si se cobra por usar las carreteras, la temperatura aumentará en verano hasta un nivel insoportable. Este verano la temperatura está resultando ser bastante agradable. La conclusión es ineludible: la contaminación es aceptable». ¿Se corresponde lo publicado por este medio con lo dicho realmente por el ministerio?

[Cubit 14], [EFO 20.5.2022:1] (argumento $\mathcal{B}$), [SEL 1:3] (argumento $\mathcal{B}$). *Cfr.* CRILLY [59]: capítulo 16: Lógica (págs. 72–73).

Resolución.—

0. *Argumento* ($\mathcal{B}$): Si hay menos coches en las carreteras, entonces la contaminación será aceptable. Hay menos coches en las carreteras o hay que pagar por usar las carreteras, o ambas cosas. Si hay

---

[63] Truth Table Generator (https://mrieppel.net/prog/truthtable.html), de Michael RIEPPEL (https://mrieppel.net/).

[64] Logic Calculator (https://www.erpelstolz.at/gateway/TruthTable.html), de Christian GOTTSCHALL (https://www.erpelstolz.at/christian/homepage-uk.html), en Gateway to Logic (https://www.erpelstolz.at/gateway/); en la versión de Logic Calculator del lado del servidor (https://www.erpelstolz.at/gateway/formular-uk-zentral.html) debemos elegir en el desplegable «Task to be performed» [Tarea para ser realizada], «Detailed truth table (showing intermediate results)» [Tabla de verdad detallada (mostrando resultados intermedios)]; y, cuidado, porque este artefacto en línea no distingue mayúsculas de minúsculas; por otro lado, en él, `W` (VERUM) denota una fórmula válida y `F` (FALSUM) una fórmula insatisfactible; además, `&` y `|` designan la conjunción y la disyunción, respectivamente (sobre lo que puede hacer, *vid.* https://www.erpelstolz.at/gateway/server-taskhelp.html y sobre la sintaxis, *vid.* https://www.erpelstolz.at/gateway/server-languagehelp.html).

[65] Pudiésemos utilizar el manual de referencia de Sage —*vid.* https://doc.sagemath.org/html/en/reference/logic/index.html (o https://doc.sagemath.org/pdf/en/reference/logic)— (código que ya sabemos que pudiésemos ejecutar en la celda libre de computación de SageMath [https://sagecell.sagemath.org/]), aunque con la biblioteca sugerida parece no poder utilizarse directamente la fórmula válida ni la insatisfactible (si bien sí existe otra posibilidad en Sage para hacerlo —¡investiguémoslo! [✍]—).

[66] El artículo «Truth table» (https://rosettacode.org/wiki/Truth_table), en *Rosetta Code* (https://rosettacode.org/wiki/Rosetta_Code) —una buena crestomatía de programación—, recoge los códigos de las implementaciones de una tabla de verdad en 48 lenguajes de programación.

que pagar por usar las carreteras, entonces la temperatura aumentará en verano hasta un nivel insoportable. La temperatura no ha aumentado en verano hasta un nivel insoportable. Luego, la contaminación es aceptable.

(Que el verano sea agradable es contrario a que la temperatura en verano alcance un calor insoportable).

1. *Formalización de $\mathcal{B}$ en lógica de juntores*.

   - *Variables proposicionales*.

     Siendo el universo de discurso el de la realidad pasada, presente y futura del territorio en cuestión, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

     $c \leftrightharpoons$ Hay menos coches en las carreteras;

     $p \leftrightharpoons$ La contaminación será aceptable;

     $s \leftrightharpoons$ Hay que pagar por usar las carreteras;

     $d \leftrightharpoons$ La temperatura atmosférica descenderá;

     $h \leftrightharpoons$ La temperatura aumentará en verano hasta un nivel insoportable.

   - *Esquema argumental*:

     Si se supone c, se sigue p.
     Se tiene $c \vee s$.
     Si se supone s, se sigue h.
     Se tiene $\neg h$.

     $\therefore$ Se sigue p.

     (Que el verano sea agradable es contrario a que la temperatura en verano alcance un calor insoportable).

   - *Forma lógica*.

     Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2, \phi_3\} = \{c \to p, c \vee s, s \to h, \neg h\}$ y la conclusión ψ, a saber, p. La fórmula correspondiente a $\mathcal{B}$ en lógica de juntores es $(c \to p) \wedge (c \vee s) \wedge (s \to h) \wedge \neg h \to p$. Llamémosla B.

2. *Demostración de si $\mathcal{B}$ es o no es un argumento válido*.

   I. *Resolución de $\mathcal{B}$ utilizando tablas de verdad como estrategia de verificación*.

   Utilizando tablas de verdad como estrategia de verificación,

c	h	p	s	((((c	$\to$	p)	$\wedge$	(c	$\vee$	s))	$\wedge$	(s	$\to$	h))	$\wedge$	$\neg$	h)	$\boxed{\to}$	p
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	1	1	1
1	1	1	0	1	1	1	1	1	1	0	1	0	1	1	0	0	1	1	1
1	1	0	1	1	0	0	0	1	1	1	0	1	1	1	0	0	1	1	0
1	1	0	0	1	0	0	0	1	1	0	0	0	1	1	0	0	1	1	0
1	0	1	1	1	1	1	1	1	1	1	0	1	0	0	0	1	0	1	1
1	0	1	0	1	1	1	1	1	1	0	1	0	1	0	1	1	0	1	1
1	0	0	1	1	0	0	0	1	1	1	0	1	0	0	0	1	0	1	0
1	0	0	0	1	0	0	0	1	1	0	0	0	1	0	0	1	0	1	0
0	1	1	1	0	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1
0	1	1	0	0	1	1	0	0	0	0	0	0	1	1	0	0	1	1	1
0	1	0	1	0	1	0	1	0	1	1	1	1	1	1	0	0	1	1	0
0	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0
0	0	1	1	0	1	1	1	0	1	1	0	1	0	0	0	1	0	1	1
0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	1	0	1	1
0	0	0	1	0	1	0	1	0	1	1	0	1	0	0	0	1	0	1	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	1	0

resulta que todas las interpretaciones son modelos, por lo que B es una fórmula válida, $\mathcal{B}$ un argumento válido e, igualmente, la argumentación es válida.

II. *Identificación del conjunto* Γ.

Al ser válida la argumentación, elegimos no hacerlo, si bien optativamente pudiésemos como actividad práctica de RAA (*cfr.* actividad 1.12 [pág. 136 de esta edición]).

III. *Resolución de* $\mathcal{A}$ *utilizando las tablas de verdad como estrategia de refutación*.

Lo mismo que el anterior (*cfr.* actividad 1.12 [pág. 136 de esta edición]).

3. No procede (la argumentación es válida).

4. No procede (la argumentación es válida).

5. No procede (la argumentación es válida). 

Actividad 1.12

Del ejemplo anterior, II., identifiquemos el conjunto Γ, y III., resolvamos $\mathcal{A}$ utilizando las tablas de verdad como estrategia de refutación.

Ejemplo 97

> «Utilizaremos ambas componentes software sólo si a igual número de peticiones su capacidad de respuesta es la misma. Cuidado, insistimos, que el número de peticiones sea el mismo, no sólo que respondan por igual. Pero entonces, de todo lo anterior, se deduce que no es cierto que se vayan a utilizar ambas componentes».
>
> [EPF 14.5.2019:1a], [EPF 14.5.2019:1b2] (por tablas de verdad como estrategia de refutación).

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si utilizamos ambas componentes software, entonces si ambas componentes software reciben igual número de peticiones, entonces ambas componentes software tienen la misma capacidad de respuesta. Ambas componentes software reciben igual número de peticiones y ambas componentes software tienen la misma capacidad de respuesta. Luego, no utilizamos ambas componentes software.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

   - *Variables proposicionales*:

     Siendo el universo de discurso el de las componentes software, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

     $p \leftrightharpoons$ Utilizamos ambas componentes software;

     $q \leftrightharpoons$ Ambas componentes software reciben igual número de peticiones;

     $r \leftrightharpoons$ Ambas componentes software tienen la misma capacidad de respuesta.

   - *Esquema argumental*:

     Si se supone p, se sigue que si se supone q, se sigue r.
     Se tiene q y r.

     ∴ Se sigue no p.

   - *Forma lógica*.

     Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{p \to (q \to r), q \wedge r\}$ y la conclusión ψ, a saber, $\neg p$.

     La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es

     $$(p \to (q \to r)) \wedge (q \wedge r) \to \neg p.$$

     Llamémosla A.

2. *Demostración de si $\mathcal{A}$ es o no es un argumento válido.*

   I. *Resolución de $\mathcal{A}$ utilizando tablas de verdad como estrategia de verificación.*

   Demostremos que el argumento A no es lógicamente válido. Para ello, utilicemos las tablas de verdad como estrategia de verificación.

p	q	r	$((p$	$\to$	$(q$	$\to$	$r))$	$\land$	$(q$	$\land$	$r))$	$\boxed{\to}$	$\neg$	p
1	1	1	1	1	1	1	1	1	1	1	1	0	0	1
1	1	0	1	0	1	0	0	0	1	0	0	1	0	1
1	0	1	1	1	0	1	1	0	0	0	1	1	0	1
1	0	0	1	1	0	1	0	0	0	0	0	1	0	1
0	1	1	0	1	1	1	1	1	1	1	1	1	1	0
0	1	0	0	1	1	0	0	0	1	0	0	1	1	0
0	0	1	0	1	0	1	1	0	0	0	1	1	1	0
0	0	0	0	1	0	1	0	0	0	0	0	1	1	0

   Al existir un contramodelo para A, apreciamos que ésta es una fórmula no válida, por lo tanto, $\mathcal{A}$ es un argumento no válido e, igualmente, la argumentación es no válida.

   II. *Identificación del conjunto Γ.*

   Identificamos la estructura de $\mathcal{A}$ con ser $\phi_0 \land \phi_1 \to \psi$ una fórmula válida. Por el teorema 1.2 (pág. 71 de esta edición) sabemos que w es un contramodelo para dicha fórmula si, y sólo si, w es un modelo para Γ, donde $\Gamma = \Phi \cup \{\neg\psi\} = \{p \to (q \to r), q \land r, p\}$.

   III. *Resolución de $\mathcal{A}$ utilizando las tablas de verdad como estrategia de refutación.*

   Estudiemos si existe una refutación para Γ —esto es, si utilizando la tabla de verdad como estrategia de refutación encontramos que la tabla para Γ es una tabla insatisfactible—, una tabla de refutación, para Γ.

   Como vimos en el apartado 2.III del ejemplo 93 (pág. 125 de esta edición), debido al teorema 1.2 (pág. 71 de esta edición), es posible estudiar la tabla para Γ, esto es, la tabla para $(p \to (q \to r)) \land (q \land r) \land p$, a partir de su verdad (*cfr.* 2.III.A de dicho ejemplo) o, equivalentemente, la tabla para $(p \to (q \to r)) \land (q \land r) \to \neg p$, a partir de su falsedad (*cfr.* 2.III.B de dicho ejemplo).

   Estudiamos esta última en el caso presente.

   Nuestro punto de comienzo es la falsedad de $(p \to (q \to r)) \land (q \land r) \to \neg p$, esto es, su negación, $\neg((p \to (q \to r)) \land (q \land r) \to \neg p)$, lo cual supone la negación de la conclusión, esto es, $\neg p$ es falsa, es decir, p es verdadera; por otra parte, de la segunda premisa, ser ésta verdadera es ser la conjunción verdadera y, por lo tanto, ambos conjuntos, q y r; en definitiva, $[\![p]\!] = 1$, $[\![q]\!] = 1$ y $[\![r]\!] = 1$,

p	q	r	$((p$	$\rightarrow$	$(q$	$\rightarrow$	$r))$	$\wedge$	$(q$	$\wedge$	$r))$	$\boxed{\rightarrow}$	$\neg$	p
1	1	1	1	1	1	1	1	1	1	1	1	0	0	1

En definitiva, hemos encontrado un modelo para Γ, o lo que es equivalente, un contramodelo para $\mathcal{A}$, por lo que $\mathcal{A}$ no es un argumento válido y, en definitiva, la argumentación es no válida.

3. *Identificación de los modelos para Γ que proporciona la tabla para Γ.*

Vía las tablas de verdad, tanto como estrategia de verificación como de refutación, concluimos que la interpretación I_{111} es el único modelo para Γ (por ser el único contramodelo para A).

4. *Demostración de que los modelos lo son para Γ.*

Demostremos que I_{111} es un modelo para Γ; para ello, estudiemos la valoración de verdad de las fórmulas de Γ con dicha interpretación:

p	q	r	p	$\rightarrow$	$(q$	$\rightarrow$	$r)$	q	$\wedge$	r	p
1	1	1	1	$\boxed{1}$	1	1	1	1	$\boxed{1}$	1	$\boxed{1}$

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

Una contraargumentación construida a partir de I_{111} sería la siguiente.

Caso de que utilicemos ambas componentes software, ambas reciban igual número de peticiones y ambas tengan la misma capacidad de respuesta, se satisface la primera premisa (es un condicional con antecedente y consecuente verdaderos [éste último por ser una conjunción de sendos conjuntos verdaderos]) y también se satisface la segunda premisa (ambas reciben igual número de peticiones y ambas tienen la misma capacidad de respuesta), pero no se satisface la conclusión (es falso que no utilicemos ambas componentes software, pues las utilizamos). ■

Actividad 1.13

«La condición era que sólo si ibas tú iría tu hermana o tu amiga. No fue tu amiga. Así que, fuiste tú o tu hermana». ¿Es válida esta argumentación? (Sigamos el esquema de la pág. 124 de esta edición).

[Cubit 3], [SEL 1:1].

Con miras a su resolución.— La fórmula correspondiente a esta argumentación en la lógica de juntores es $(h \vee a \rightarrow t) \wedge \neg a \rightarrow (t \vee h)$, donde las variables proposicionales son: $h \leftrightharpoons$ Va tu hermana; $a \leftrightharpoons$ Va tu amiga; $t \leftrightharpoons$ Vas tú. Utilizando las tablas de verdad como estrategia de refutación, en la búsqueda de los modelos para $((h \vee a \rightarrow t) \wedge \neg a) \wedge \neg(t \vee h)$ —la negación de $(h \vee a \rightarrow t) \wedge \neg a \rightarrow (t \vee h)$—, con las variables en el orden h, a, t: el hecho de que $(h \vee a \rightarrow t)$ deba ser verdadero, descarta las interpretaciones I_{110}, I_{100} e I_{010}; el hecho de que $\neg a$ deba ser verdadero, descarta las interpretaciones I_{111}, I_{110}, I_{011} e I_{010}, y el hecho de que $(t \vee h)$ deba ser falso, descarta las interpretaciones I_{111}, I_{101}, I_{110}, I_{100}, I_{011} e I_{001}; en definitiva, el único

modelo para $((h \vee a \to t) \wedge \neg a) \wedge \neg(t \vee h)$ es I_{000}. La expresión en español de la contraargumentación proporcionada por este modelo para $((h \vee a \to t) \wedge \neg a) \wedge \neg(t \vee h)$ es «Si no va tu hermana ni tu amiga ni tú, se satisface que va tu hermana o tu amiga sólo si vas tú y también que tu amiga no va, esto es, se satisfacen las premisas, pero no se satisface la conclusión porque ni vas tú ni va tu hermana.» Resta que completemos la resolución atendiendo al esquema de la pág. 124 de esta edición).

Actividad 1.14

«Una inteligencia artificial es o no es. El ser humano es, conque una inteligencia artificial también es. Luego, no es verdad eso que dicen de que una inteligencia artificial no es porque el ser humano es». ¿Es válida esta argumentación? (Sigamos el esquema de la pág. 124 de esta edición).

[Cubit 1].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $(p \vee \neg p) \wedge (q \to p) \to \neg(q \to \neg p)$, donde las variables proposicionales son: $p \leftrightharpoons$ Una inteligencia artificial es; $q \leftrightharpoons$ El ser humano es. Resta que completemos la resolución atendiendo al esquema de la pág. 124 de esta edición.

Actividad 1.15

«Lo haré, a menos que tú me lo impidas. Tampoco lo haré si llegamos a un acuerdo. En definitiva, lo haré si no llegamos a un acuerdo o tú me lo impides». ¿Es válida esta argumentación? (Sigamos el esquema de la pág. 124 de esta edición).

[Cubit 6].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $(p \vee q) \wedge (r \to \neg p) \to ((\neg r \vee q) \to p)$, donde las variables proposicionales son: $p \leftrightharpoons$ Lo haré; $q \leftrightharpoons$ Me lo impides; $r \leftrightharpoons$ Llegamos a un acuerdo. Con respecto a «a menos que», observemos que podemos reescribir equivalentemente: «Sucederá p, a menos que suceda q» $\equiv$ «Si no sucede q, sucederá p» $[\neg q \to p] \equiv$ «O sucede p o sucede q o ambas» $[p \vee q]$. (La primera equivalencia sucede en nuestra lengua, la segunda en la lógica de juntores, a saber, el principio de Filón, junto a la conmutativa de la disyunción). Resta que completemos la resolución atendiendo al esquema de la pág. 124 de esta edición.

Actividad 1.16

«Si quien accede ha ingresado correctamente las credenciales, entonces: si el sistema ha verificado la autenticidad de quien accede, entonces quien accede tiene permisos de administración. Si quien accede puede además acceder a la configuración avanzada del sistema, entonces: si quien accede no ha ingresado correctamente las credenciales, entonces el sistema ha verificado la autenticidad de quien accede. Si quien accede tiene permisos de administración, entonces: el sistema ha verificado la autenticidad de quien accede y quien accede puede además acceder a la configuración avanzada del sistema. Por lo tanto, si quien accede tiene permisos

de administración, entonces quien accede ha ingresado correctamente las credenciales». ¿Es válida esta argumentación? (Sigamos el esquema de la pág. 124 de esta edición).

[Cubit 16].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $(p \rightarrow (q \rightarrow r)) \wedge (s \rightarrow (\neg p \rightarrow q)) \wedge (r \rightarrow (q \wedge s)) \rightarrow (r \rightarrow p)$, donde las variables proposicionales son: p ≒ Quien accede ha ingresado correctamente las credenciales; q ≒ El sistema ha verificado la autenticidad de quien accede; r ≒ Quien accede tiene permisos de administración; s ≒ Quien accede puede además acceder a la configuración avanzada del sistema. Resta que completemos la resolución atendiendo al esquema de la pág. 124 de esta edición —si bien, en el entretanto, pudiésemos utilizar, por ejemplo, el artefacto en línea Wolfram|Alpha[67], con la petición `tabla de verdad ((p implies (q implies r)) and (s implies (not p implies q)) and (r implies (q and s))) implies (r implies p)`, observando que es una fórmula no válida y que el único contramodelo para ella es $\langle p, q, r, s\rangle \leftarrow \langle 0, 1, 1, 1\rangle$, abreviadamente, I_{0111}—.

Actividad 1.17

«Si el servidor está encendido, el cráquer ejecutará secuencias maliciosas de comandos y escaneará los puertos abiertos. Si ejecuta secuencias maliciosas de comandos y encuentra el cortafuegos desactivado, entrará, instalará programas malignos, pero le bloquearé la dirección IP. Si escanea los puertos abiertos y encuentra el cortafuegos activado, se enfurecerá, lanzará un ataque de denegación de servicio y le bloquearé la dirección IP. Así pues, si el servidor está encendido y el cráquer encuentra el cortafuegos activado o desactivado, le bloquearé la dirección IP». ¿Es válida esta argumentación? (Sigamos el esquema de la pág. 124 de esta edición —igual que en el ejemplo 94 (pág. 128 de esta edición), resolveremos 2.III por reducción al absurdo—).

[Cubit 19].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $(s \rightarrow (c \wedge p)) \wedge ((c \wedge f) \rightarrow (i \wedge m \wedge b)) \wedge ((p \wedge \neg f) \rightarrow (e \wedge d \wedge b)) \rightarrow ((s \wedge (f \vee \neg f)) \rightarrow b)$, donde las variables proposicionales son: s ≒ El servidor está encendido; c ≒ El cráquer ejecuta secuencias maliciosas de comandos; p ≒ El cráquer escanea los puertos abiertos; f ≒ El cortafuegos está desactivado; i ≒ El cráquer entra en el sistema; m ≒ El cráquer instala programas malignos; b ≒ Bloqueo la dirección IP del cráquer; e ≒ El cráquer se enfurece; d ≒ El cráquer lanza un ataque de denegación de servicio. Resta que completemos la resolución atendiendo al esquema de la pág. 124 de esta edición, resolviendo 2.III por reducción al absurdo, según el enunciado —si bien, en el entretanto, pudiésemos emplear las tablas de verdad como estrategia verificadora, utilizando, por ejemplo, el artefacto en línea Truth Table Generator[68], con la petición `(((s > (c & p)) & ((c & f) > ((i & m) & b))) & ((p & ∼ f) > ((e & d) & b))) > ((s & (f v ∼ f)) > b)`, observando que es una fór-

[67] https://www.wolframalpha.com/.
[68] https://mrieppel.net/prog/truthtable.html.

mula válida, o las tablas analíticas/semánticas (TA/S)[69], utilizando, por ejemplo, el artefacto en línea Truth Tree Solver[70], que con la petición `∼ ((((S ⊃ (C & P)) & ((C & F) ⊃ ((I & M) & B))) & ((P & ∼ F) ⊃ ((E & D) & B))) ⊃ ((S & (F ∨ ∼ F)) ⊃ B))`, observando que genera un árbol insatisfactible, lo que corresponde a que la fórmula sea válida—.

Observación 1.8.2.— También, más adelante, resolveremos el ejemplo 97 (pág. 137 de esta edición) mediante tablas analíticas/semánticas (TA/S) (*cfr. infra* ejemplo 167 [pág. 325 de esta edición]).

Actividad 1.18

«Las neuronoides se verán obligadas a reprogramarse agresivamente y dejarán sin protección las áreas de interés si, y sólo si, quienes revisan el sistema introducen un nuevo vector de entrada o los organoides del laboratorio no consiguen desarrollar una red de comunicación. Pero si quienes dirigen cumplen lo prometido o quienes revisan el sistema no introducen un nuevo vector de entrada, las neuronoides únicamente entablarán una conversación entre ellas y, en caso de que quienes dirigen les contacten amistosamente, participarán con ellas en una mesa de debate. O es cierto que quienes dirigen les contactan amistosamente o se conservan las protecciones en todas las áreas de interés. Si quienes dirigen participan con las neuronoides en una mesa de debate, las conclusiones de ésta serán públicamente compartidas. No es cierto que se conserven las protecciones en todas las áreas de interés o que quienes dirigen no cumplen lo prometido. Así pues, si los organoides del laboratorio no consiguen desarrollar una red de comunicación, las neuronoides se verán obligadas a reprogramarse agresivamente y las conclusiones de la mesa de debate serán públicamente compartidas.». ¿Es válida esta argumentación? (Sigamos el esquema de la pág. 124 de esta edición).

[Cubit 7].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $(p \wedge q \leftrightarrow r \vee \neg s) \wedge (t \vee \neg r \rightarrow u) \wedge (w \rightarrow m) \wedge (w \vee n) \wedge (m \rightarrow \tilde{n}) \wedge \neg(n \vee \neg t) \rightarrow (\neg s \rightarrow p \wedge \tilde{n})$, donde las variables proposicionales son: $p \leftrightharpoons$ Las neuronoides se verán obligadas a reprogramarse agresivamente; $q \leftrightharpoons$ Las neuronoides dejarán sin protección las áreas de interés; $r \leftrightharpoons$ Quienes revisan el sistema introducen un nuevo vector de entrada; $s \leftrightharpoons$ Los organoides del laboratorio no consiguen desarrollar una red de comunicación; $t \leftrightharpoons$ Quienes dirigen cumplen lo prometido; $u \leftrightharpoons$ Las neuronoides únicamente entablarán una conversación entre ellas; $w \leftrightharpoons$ Quienes dirigen contactan amistosamente con las neuronoides; $m \leftrightharpoons$ Quienes dirigen participan con con las neuronoides en una mesa de debate; $n \leftrightharpoons$ Se conservan las protecciones en todas las áreas de interés; $\tilde{n} \leftrightharpoons$ Las conclusiones de la mesa de debate serán públicamente compartidas. Resta que completemos la resolución atendiendo al esquema de la pág. 124 de esta edición. En el entretanto, pudiésemos emplear las tablas de

[69] *Vid. infra* § 3.3 (pág. 274 de esta edición).
[70] https://www.formallogic.com/en/truth-tree-solver.

verdad como estrategia verificadora; por ejemplo, utilizando la celda libre de computación de SageMath[71]:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
# referencia: https://doc.sagemath.org/html/en/reference/logic/index.html
f = propcalc.formula("(p & q <-> r | ~ s) & (t | ~ r -> u) & (w -> m) & (w | n) & (m -> z) & ~
    ↪ (n | ~ t) -> (~ s -> p & z)") # introducimos la fórmula (ñ representada por z)
show(f) # mostramos la fórmula
print(f.truthtable()) # mostramos su tabla de verdad
show(f.is_tautology()) # mostramos si es una fórmula válida
show(f.is_satisfiable()) # mostramos si es una fórmula satisfactible
show(f.is_contradiction()) # mostramos si es una fórmula insatisfactible
```

§ 1.9 Conexión aritmética

Pudiésemos adoptar el punto de vista de los juntores como functores veritativos, por ejemplo, juntores monádicos ($*^1$) y diádicos ($*^2$),

$$*^1 : \mathcal{F}_0 \longrightarrow \{0,1\},$$
$$*^2 : \mathcal{F}_0 \times \mathcal{F}_0 \longrightarrow \{0,1\},$$

así, distribuidas las atribuciones veritativas para dos variables proposicionales p y q, es posible expresar las composiciones utilizando la restricción de la función signo a $\{0,1\}$,

$$\begin{array}{rccl} \operatorname{sgn}: & \{0,1\} & \longrightarrow & \{0,1\} \\ & x & \longmapsto & \operatorname{sgn}(x) = \begin{cases} 0 & \text{si} \quad x \leq 0 \\ 1 & \text{si} \quad x > 0 \end{cases} \end{array}$$

y las funciones aritméticas habituales entre números; en particular, a modo de ejemplo y por ser muy habituales, estas definiciones de las composiciones generadas por los juntores de la base $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$ son:

$$\neg p \leftrightharpoons \operatorname{sgn}(1-p),$$

esto es, si p si, y sólo si $p = 1$, entonces

$$\neg p \text{ si, y sólo si } p = 0;$$

$$\begin{aligned} p \vee q &\leftrightharpoons \operatorname{sgn}(p+q) \\ &= \begin{cases} 0 & \text{si } p+q \leq 0 \\ 1 & \text{si } p+q > 0, \end{cases} \end{aligned}$$

[71] *Vid.* https://sagecell.sagemath.org/.

esto es,

$$p \vee q \text{ si, y sólo si } p + q > 0;$$

$$\begin{aligned} p \wedge q &\fallingdotseq \operatorname{sgn}(p \cdot q) \\ &= \begin{cases} 0 & \text{si } p \cdot q \leq 0 \\ 1 & \text{si } p \cdot q > 0 \end{cases} \\ &= p \cdot q, \end{aligned}$$

esto es,

$$p \wedge q \text{ si, y sólo si } p \cdot q > 0,$$

claro que también,

$$p \wedge q \text{ si, y sólo si } p + q = 2;$$

$$\begin{aligned} p \to q &\fallingdotseq \operatorname{sgn}(1 - (p - q)) \\ &= \begin{cases} 0 & \text{si } p - q > 0 \\ 1 & \text{si } p - q \leq 0, \end{cases} \end{aligned}$$

esto es,

$$p \to q \text{ si, y sólo si } p - q \leq 0;$$

$$\begin{aligned} p \leftrightarrow q &\fallingdotseq \operatorname{sgn}((1 - (p - q)) \cdot (1 - (q - p))) \\ &= \operatorname{sgn}((1 - (p - q)) \cdot (1 + (p - q))) \\ &= \operatorname{sgn}(1^2 - (p - q)^2) \\ &= \begin{cases} 0 & \text{si } p - q \neq 0 \\ 1 & \text{si } p - q = 0, \end{cases} \end{aligned}$$

esto es,

$$p \leftrightarrow q \text{ si, y sólo si } p - q = 0.$$

Algunas descripciones aritméticas de sus valores de verdad, en realidad, descripciones de su comportamiento veritativo-funcional, son:

$$\begin{aligned} [\![\neg p]\!] &\fallingdotseq 1 - [\![p]\!]; \\ [\![p \vee q]\!] &\fallingdotseq \text{máx}\{[\![p]\!], [\![q]\!]\} \end{aligned}$$

$$
\begin{aligned}
&= \text{mín}\{1, [\![p]\!] + [\![q]\!]\}; \\
[\![p \wedge q]\!] &\coloneqq [\![p]\!] \cdot [\![q]\!] \\
&= \text{mín}\{[\![p]\!], [\![q]\!]\} \\
&= \text{máx}\{0, [\![p]\!] + [\![q]\!] - 1\}; \\
[\![p \rightarrow q]\!] &\coloneqq \text{mín}\{1, 1 + [\![q]\!] - [\![p]\!]\} \\
&= 1 - [\![p]\!](1 - [\![q]\!]); \\
[\![p \leftrightarrow q]\!] &\coloneqq [\![p]\!] \cdot [\![q]\!] + [\![\neg p]\!] \cdot [\![\neg q]\!] \\
&= 1 - |[\![p]\!] - [\![q]\!]|.
\end{aligned}
$$

En ellas, distribuyendo las atribuciones veritativas para las variables p y q, es decir, sustituyendo los pares ordenados $\langle p, q\rangle$ por sus posibles valores $\langle 1, 1\rangle$, $\langle 1, 0\rangle$, $\langle 0, 1\rangle$ y $\langle 0, 0\rangle$, esto es, por las interpretaciones, se obtienen los valores de verdad de las fórmulas.

Observación 1.9.0.— Esta conexión aritmética es en ambos sentidos. A modo de ejemplo, pudiésemos escribir la función segmentada

$$
\begin{aligned}
f: \quad \mathbb{Q} &\longrightarrow \mathbb{Q} \\
x &\longmapsto f(x) = \begin{cases} 0 & \text{si} \quad x \leq 0, \\ x & \text{si} \quad 0 < x < 1, \\ 1 & \text{si} \quad 1 \leq x, \end{cases}
\end{aligned}
$$

como

$$f(x) = (x \leq 0) \cdot 0 + (0 < x \wedge x < 1) \cdot x + (1 \leq x) \cdot 1.$$

En efecto:

- si $x \leq 0$, $f(0) = (0 \leq 0) \cdot 0 + (0 < 0 \wedge 0 < 1) \cdot 0 + (1 \leq 0) \cdot 1 = 1 \cdot 0 + (0 \wedge 1) \cdot 0 + 0 \cdot 1 = 1 \cdot 0 + 0 \cdot 0 + 0 \cdot 1 = 0$;
- si $0 < x < 1$, $f(x) = 0 \cdot 0 + 1 \cdot x + 0 \cdot 1 = x$;
- si $1 \leq x$, $f(x) = 0 \cdot 0 + 0 \cdot x + 1 \cdot 1 = 1$.

§ 1.10 Implicación lógica

Definición 1.18.— Sean ψ una fórmula y Φ un conjunto de fórmulas. Decimos que Φ *implica lógicamente* (o, sinónimamente, *implica tautológicamente*) a ψ (o, sinónimamente, que ψ es *consecuencia lógica* o que se *deduce*, *deriva* o *infiere semánticamente* de Φ) y lo designamos por $\Phi \vDash \psi$, precisamente si todo modelo para Φ es un modelo para ψ; en otras palabras, precisamente si $\mathcal{M}(\Phi) \cap \mathcal{M}(\psi) = \mathcal{M}(\Phi)$. En definitiva,

$$\Phi \vDash \psi \coloneqq \mathcal{M}(\Phi) \subseteq \mathcal{M}(\psi).$$

Observación 1.10.0.— Al símbolo $\models$ le llamamos *deductor semántico* (o, sinónimamente, *consecutor*). Aunque en algunos textos se usan los símbolos $\models$ y $\Rightarrow$ indistintamente, reservamos este último para representar el «si ..., entonces ...» (o, sinónimamente, al «...sólo si ...» o al «...implica ...») de nuestra *lengua natural*, a diferencia de $\rightarrow$, que es el condicional material de la *lógica ordinaria*.

En otros textos se diferencia entre *implicación lógica* ($\Rightarrow$) e *implicación tautológica* ($\models$).

En una escala desde el *lenguaje objeto* a los diferentes niveles de *metalenguaje* empleados: $\rightarrow$, $\leftarrow$, $\leftrightarrow$ se sitúan en el nivel cero (lenguaje objeto $\mathcal{L}_0$); $\vdash$, $\dashv$, $\dashv\vdash$, $\models$, $\Dashv$, $\equiv$ en el nivel uno de metalenguaje de $\mathcal{L}_0$, y $\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$ en un nivel dos de metalenguaje, el lenguaje lógico-matemático (*cfr. infra* cuadro 2.0 [pág. 179 de esta edición]).

Ejemplo 98

Demostremos que se satisface que $\{p \wedge q\} \models p \vee q$.

Resolución.— Designando por I_{11}, I_{10}, I_{01}, I_{00} las diferentes interpretaciones para las variables proposicionales p y q, las tablas de verdad de $p \wedge q$ y $p \vee q$ muestran que la única interpretación que es un modelo para $p \wedge q$ es I_{11} y que las interpretaciones que son modelos para $p \vee q$ son I_{11}, I_{10} y I_{01}; de aquí que todo modelo para $p \wedge q$ lo es también para $p \vee q$. ■

Observación 1.10.1.— Como curiosidad: en inglés, la implicación lógica también es conocida como *entailment*; por ello, en inglés, $\Phi \models \psi$ se lee Φ *entails* ψ (o ψ *is entailed by* Φ).

Que Φ no implique lógicamente ψ se nota $\Phi \not\models \psi$.

Ejemplo 99

Demostremos que se satisface que $\{p \vee q\} \not\models p \wedge q$.

Resolución.— En efecto, por el ejemplo anterior sabemos que la única interpretación que es un modelo para $p \wedge q$ es I_{11} y que las interpretaciones que son modelos para $p \vee q$ son I_{11}, I_{10} y I_{01}, por lo que I_{10} y I_{01} son modelos para $p \vee q$ que no lo son para $p \wedge q$. ■

Al no existir ninguna fórmula en el conjunto vacío $\emptyset$ que sea falsa en alguna interpretación, admitimos que toda interpretación es un modelo para $\emptyset$, por lo que $\emptyset \models \phi$ significa que todas las interpretaciones son un modelo para ϕ, esto es, que ϕ es una fórmula válida. De aquí que el hecho de ser ϕ una fórmula válida lo designemos por $\models \phi$.

Observemos que si ninguna interpretación satisface a todas las fórmulas de Φ (por ejemplo, si $\Phi = \{\phi, \neg\phi\}$), entonces Φ implica lógicamente toda fórmula, y esto porque para ninguna puede encontrarse un contraejemplo[72], una interpretación que sea modelo para Φ y no lo sea para la fórmula.

Observación 1.10.2.— De aquí en adelante, nos tomamos la licencia de expresar $\{\phi\} \vDash \psi$ simplemente por $\phi \vDash \psi$.

Teorema 1.10
Sean ψ una fórmula y Φ un conjunto de fórmulas. Entonces,

$$\Phi \vDash \psi \text{ si, y sólo si, } \Phi \cup \{\neg\psi\} \text{ es insatisfactible.}$$

Observemos que $\phi \vDash \psi$ es una afirmación que dice que ϕ implica lógicamente a ψ, expresando una relación causa-efecto (esto es, que si lo afirmado por ϕ es verdadero, también lo es lo afirmado por ψ), mientras que $\phi \to \psi$ es una «simple» fórmula, o a lo sumo, un esquema de fórmula. No obstante, existen varias relaciones entre ellos.

Teorema 1.11
Sean ϕ y ψ dos fórmulas y Φ un conjunto de fórmulas. Entonces,

$$\Phi \cup \{\phi\} \vDash \psi \text{ si, y sólo si, } \Phi \vDash \phi \to \psi.$$

Teorema 1.12
Sean ϕ y ψ dos fórmulas. Entonces,

$$\phi \vDash \psi \text{ si, y sólo si, } \vDash \phi \to \psi.$$

Precisamente el hecho de que $\phi \to \psi$ sea una fórmula válida justifica que la expresión $\phi \vDash \psi$ puede ser usada como esquema de un *argumento válido*.

De manera similar que en la definición de conjunto satisfactible de fórmulas, más ahora en la definición de $\Phi \vDash \psi$, la posibilidad de un conjunto Φ infinito, pudiese provocarnos cierta inquietud, no obstante el siguiente teorema, una versión equivalente del teorema de compacidad, se encarga de despejarla por completo.

Teorema 1.13 (Teorema de compacidad)
Sea ψ una fórmula y Φ un conjunto de fórmulas. Entonces,

$$\Phi \vDash \psi \text{ si, y sólo si, } \Phi_0 \subseteq \Phi,\ \Phi_0 \text{ finito, tal que } \Phi_0 \vDash \psi.$$

[72] *Cfr. infra* § 7.7 (pág. 470 de esta edición).

Cuando el conjunto de fórmulas es finito, $\Phi = \{\phi_0, \phi_1, \ldots, \phi_n\}$, es posible reescribir equivalentemente el argumento válido que representa $\Phi \vDash \psi$ en cualquiera de las siguientes formas:

- $\Phi \vDash \psi$,
- $\{\phi_0, \phi_1, \ldots, \phi_n\} \vDash \psi$,
- $\phi_0, \phi_1, \ldots, \phi_n \vDash \psi$,
- $\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \vDash \psi$.

Teorema 1.14
Sean $\phi_0, \phi_1, \ldots, \phi_n, \psi$ fórmulas y $\Phi = \{\phi_0, \phi_1, \ldots, \phi_n\}$, entonces las siguientes afirmaciones son equivalentes:
0. $\{\phi_0, \phi_1, \ldots, \phi_n\} \vDash \psi$,
1. $\vDash (\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n) \to \psi$,
2. $\vDash (\phi_0 \to (\phi_1 \to (\cdots \to (\phi_{n-1} \to (\phi_n \to \psi)))))$.

Teorema 1.15 (Propiedades de $\vDash$)
Sean ϕ y ψ dos fórmulas y Φ y Ψ dos conjuntos de fórmulas, cualesquiera. Se satisface:
0. $\phi \vDash \phi$; (Reflexividad de $\vDash$)
1. si $\Phi \vDash \phi$ y $\Phi \subseteq \Psi$, entonces $\Psi \vDash \phi$; (Monotonía de $\vDash$)
2. si $\Phi \vDash \phi$ y $\phi \vDash \psi$, entonces $\Phi \vDash \psi$. (Transitividad de $\vDash$)

Ejemplo 100

«Siempre que el conmutador A está cerrado, B también; o bien B está cerrado o bien C está cerrado, pero nunca ambos a la vez; siempre, bien A está cerrado, bien C está cerrado, o ambos lo están, y cuando C está cerrado, A también». ¿Qué concluimos?

[Cubit 55].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si el conmutador A está cerrado, entonces B está cerrado. B está cerrado o C está cerrado, pero no ambos. A está cerrado o C está cerrado, o ambos. Si C está cerrado, entonces A está cerrado. Luego, ¿...?

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales.*

     Siendo el universo de discurso el dominio de todos los objetos, sean las siguientes tres variables proposicionales y proposiciones simples que representan:

     $a \risingdotseq A$ está cerrado; $b \risingdotseq B$ está cerrado; $c \risingdotseq C$ está cerrado.

Esquema argumental:

Si se supone a, se sigue b.
Se tiene b o se tiene c, pero no ambas.
Se tiene a o se tiene c o ambas.
Si se supone c, se sigue a.

$\therefore$ ¿...?

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2, \phi_3\} = \{a \to b, b \veebar c, a \vee c, c \to a\}$, pero debemos hallar la conclusión ψ.

2. *Hallazgo de la conclusión y demostración de la validez del argumento*.

   Utilicemos los diagramas de Venn (1834–1923) —como ejemplificación también del *razonamiento diagramático*[73]— para representar gráficamente las cuatro premisas y así descubrir la conclusión. Lo hacemos en la figura 1.1 (pág. 150 de esta edición).

   En ella, indicamos con el conjunto vacío (∅) la seguridad de que el área donde lo escribimos es un área vacía, no hay nada. Por ejemplo, en el primer caso, $a \to b$, las áreas vacías son las correspondientes a $a \wedge \neg b \wedge c$ y $a \wedge \neg b \wedge \neg c$, lo cual es debido a que

$$(a \to b) \leftrightarrow (\neg(a \wedge \neg b \wedge c) \wedge \neg(a \wedge \neg b \wedge \neg c))$$

   es una fórmula válida. Las situaciones de ∅ en los otros tres casos se explican, respectivamente, por ser fórmulas válidas las siguientes tres fórmulas:

$$(b \veebar c) \leftrightarrow (\neg(a \wedge b \wedge c) \wedge \neg(\neg a \wedge b \wedge c) \wedge \neg(a \wedge \neg b \wedge \neg c) \wedge \neg(\neg a \wedge \neg b \wedge \neg c));$$
$$(\neg a \to c) \leftrightarrow (\neg(\neg a \wedge b \wedge \neg c) \wedge \neg(\neg a \wedge \neg b \wedge \neg c));$$
$$(c \to a) \leftrightarrow (\neg(\neg a \wedge b \wedge c) \wedge \neg(\neg a \wedge \neg b \wedge c)).$$

[73] *Vid. v. gr.* https://es.wikipedia.org/wiki/Razonamiento_diagramático.

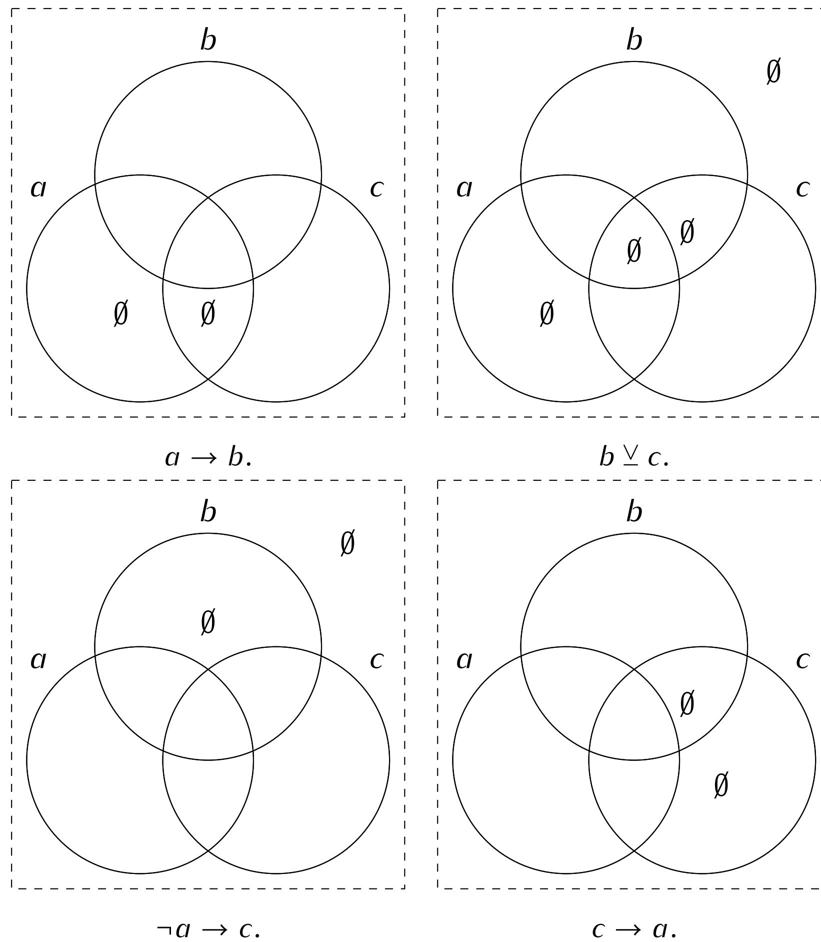
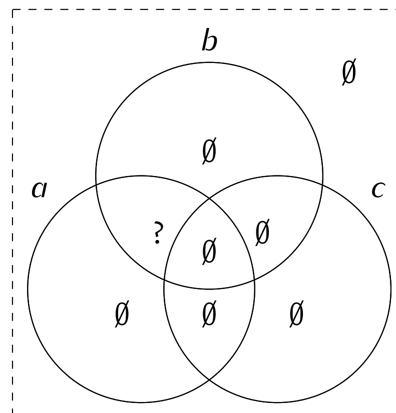


Figura 1.1.— Representación con diagramas de VENN de las cuatro premisas. En esta representación, un área con Ø designa que no hay entidades en ella, que está vacía; un área con el signo + designa la existencia de entidades en ella, esto es, que no está vacía; un área blanca designa que desconocemos si está vacía o no.

Superponiendo los cuatro diagramas, esto es, juntando la información que aportan, obtenemos el diagrama correspondiente a la conclusión, a saber, que dicha conclusión es $a \wedge b \wedge \neg c$:



El resultado de este razonamiento diagramático coincide, como era de esperar, con cualquier otro método, por ejemplo, una tabla de verdad (en la que hemos expresado la contravalencia, $b \veebar c$, como la negación de la equivalencia, $\neg(b \leftrightarrow c)$).

a	b	c	((((a	→	b)	∧	¬	(b	↔	c))	∧	(a	∨	c))	∧	(c	→	a))	**→**	((a	∧	b)	∧	¬	c)
1	1	1	1	1	1	0	0	1	1	1	0	1	1	1	0	1	1	1	1	1	1	1	0	0	1
1	1	0	1	1	1	1	1	1	0	0	1	1	1	0	1	0	1	1	1	1	1	1	1	1	0
1	0	1	1	0	0	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	0	0	0	0	1
1	0	0	1	0	0	0	0	0	1	0	0	1	1	0	0	0	1	1	1	1	0	0	0	1	0
0	1	1	0	1	1	0	0	1	1	1	0	0	1	1	0	1	0	0	1	0	0	1	0	0	1
0	1	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	1	0
0	0	1	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	0	1	0	0	0	0	0	1
0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0

■

§ 1.11 Lógica de «cámara»

Siguen algunas agrupaciones de juntores que se interrelacionan en equivalencias sin la participación de ninguno externo a la «cámara».

En la columna tabla de verdad presentan, de izquierda a derecha, las valoraciones de las fórmulas con las interpretaciones I_{11}, I_{10}, I_{01}, I_{00}.

§ 1.11.0 El solo tautología: juntor aislado, solo, único

{⊤}			
Tabla de verdad	Diagrama de Venn	Juntor	Español
1111		Tautología $\phi \top \psi$	Phi es phi y psi es psi

§ 1.11.1 El solo contradicción: juntor aislado, solo, único

{⊥}			
Tabla de verdad	Diagrama de Venn	Juntor	Español
0000		Contradicción $\phi \bot \psi$	Phi no es phi y psi no es psi

§ 1.11.2 El cuarteto DRIIn: disyuntor, replicador, implicador e incompatibilizador

$\{\vee, \leftarrow, \rightarrow, \mid\}$			
Tabla de verdad	Diagrama de Venn	Juntor	Español
1110		Disyuntor $\phi \vee \psi$ $\neg\phi \rightarrow \psi$ $\phi \leftarrow \neg\psi$ $\neg\phi \mid \neg\psi$	Phi o psi No phi sólo si psi Phi si no psi No phi y no psi son incompatibles
1101		Replicador $\phi \leftarrow \psi$ $\phi \vee \neg\psi$ $\neg\phi \rightarrow \neg\psi$ $\neg\phi \mid \psi$	Phi si psi Phi o no psi No phi sólo si no psi No phi y psi son incompatibles
1011		Implicador $\phi \rightarrow \psi$ $\neg\phi \vee \psi$ $\neg\phi \leftarrow \neg\psi$ $\phi \mid \neg\psi$	Phi sólo si psi No phi o psi No phi si no psi Phi y no psi son incompatibles
0111		Incompatibilizador $\phi \mid \psi$ $\neg\phi \vee \neg\psi$ $\phi \rightarrow \neg\psi$ $\neg\phi \leftarrow \psi$	Phi y psi son incompatibles No phi o no psi Phi sólo si no psi No phi si psi

§ 1.11.3 El sexteto AACENN: afirmador, afirmador, contravaledor, equivaledor, negador, negador

$\{\mathrm{id}_0, \mathrm{id}_1, \veebar, \leftrightarrow, \neg_1, \neg_0\}$			
Tabla de verdad	Diagrama de Venn	Juntor	Español
1100		Afirmador$_0$ $\phi\ \mathrm{id}_0\ \psi$ $\mathrm{id}\phi$ ϕ	Se satisface phi Phi
1010		Afirmador$_1$ $\phi\ \mathrm{id}_1\ \psi$ $\mathrm{id}\psi$ ψ	Se satisface psi Psi
0110		Contravaledor $\phi \veebar \psi$ $\neg\phi \veebar \neg\psi$ $\neg\phi \leftrightarrow \psi$ $\phi \leftrightarrow \neg\psi$	O bien phi o bien psi O bien no phi o bien no psi No phi es equivalente a psi Phi es equivalente a no psi
1001		Equivaledor $\phi \leftrightarrow \psi$ $\neg\phi \leftrightarrow \neg\psi$ $\neg\phi \veebar \psi$ $\phi \veebar \neg\psi$	Phi y psi son equivalentes No phi y no psi son equivalentes O bien no phi o bien psi O bien phi o bien no psi
0101		Negador$_1$ $\phi\ \neg_1\ \psi$ $\neg\mathrm{id}\psi$ $\neg\psi$	No se satisface psi No psi
0011		Negador$_0$ $\phi\ \neg_0\ \psi$ $\neg\mathrm{id}\ \phi$ $\neg\phi$	No se satisface phi No phi

§ 1.11.4 El cuarteto CDiDrNc: conjuntor, desimplicador, desreplicador y negador conjunto

$\{\wedge, \nrightarrow, \nleftarrow, \downarrow\}$			
Tabla de verdad	Diagrama de Venn	Juntor	Español
1000		Conjuntor $\phi \wedge \psi$ $\phi \nrightarrow \neg\psi$ $\neg\phi \nleftarrow \psi$ $\neg\phi \downarrow \neg\psi$	Phi y psi Phi, pero no no psi No no phi, pero psi Ni no phi ni no psi
0100		Desimplicador $\phi \nrightarrow \psi$ $\phi \wedge \neg\psi$ $\neg\phi \nleftarrow \neg\psi$ $\neg\phi \downarrow \psi$	Phi, pero no psi Phi y no psi No no phi, pero no psi Ni no phi ni psi
0010		Desreplicador $\phi \nleftarrow \psi$ $\neg\phi \wedge \psi$ $\neg\phi \nrightarrow \neg\psi$ $\phi \downarrow \neg\psi$	No phi, pero psi No phi y psi No phi, pero no no psi Ni phi ni no psi
0001		Negador conjunto $\phi \downarrow \psi$ $\neg\phi \wedge \neg\psi$ $\neg\phi \nrightarrow \psi$ $\phi \nleftarrow \neg\psi$	Ni phi ni psi No phi y no psi No phi, pero no psi No phi, pero no psi

Observación 1.11.0.— Pudiésemos pensar en este momento en la relación entre las implicaciones y replicaciones y las desimplicaciones y desreplicaciones, así,

0. por ser $\phi \wedge \psi$ equivalente a $\phi \nrightarrow \neg\psi$ también lo es a $\neg(\phi \rightarrow \neg\psi)$ y por serlo a $\neg\phi \nleftarrow \psi$ también lo es a $\neg(\neg\phi \leftarrow \psi)$ y, en definitiva, también lo es a $\neg(\phi \mid \psi)$;

1. por ser $\phi \downarrow \psi$ equivalente a $\neg\phi \nrightarrow \psi$ también lo es a $\neg(\neg\phi \rightarrow \psi)$, y por serlo a $\phi \nleftarrow \neg\psi$ también lo es a $\neg(\phi \leftarrow \neg\psi)$ y, en definitiva, también lo es a $\neg(\neg\phi \mid \neg\psi)$;

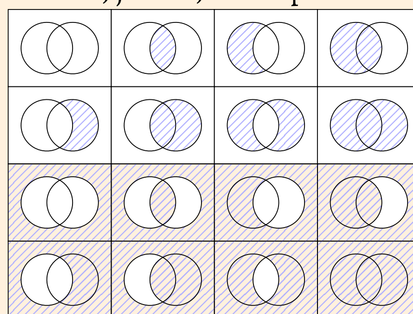
2. se tienen así para la incompatibilidad ($\mid$) y la negación conjunta ($\downarrow$) leyes similares a las de De Morgan:

   0. $\neg(\phi \mid \psi)$ si, y sólo si, $\neg\phi \downarrow \neg\psi$;

   1. $\neg(\phi \downarrow \psi)$ si, y sólo si, $\neg\phi \mid \neg\psi$.

Actividad 1.19

¿Qué tabla de verdad y, por tanto, juntor, corresponde a cada diagrama de VENN?



Actividad 1.20

¿Nos atrevemos a elegir un diagrama al azar y averiguar la tabla de verdad?

§ 1.12 Contradicción y contingencia lógicas

Entre un conjunto de fórmulas y una fórmula, además de la relación de implicación lógica, existen dos más de interés: la contradicción y la contingencia lógicas.

Definición 1.19.— Sean Φ un conjunto de fórmulas y ψ una fórmula. Decimos que Φ *contradice lógicamente* a ψ, precisamente si ningún modelo para Φ es un modelo para ψ, en otras palabras, si, y sólo si,

$$\mathcal{M}(\Phi) \cap \mathcal{M}(\psi) = \emptyset.$$

Observación 1.12.0.— Esta definición es equivalente a que se satisfaga $\Phi \models \neg\psi$.

Observación 1.12.1.— Si Φ se reduce a una fórmula, sea ésta ϕ, entonces se satisface $\phi \models \neg\psi$ y $\psi \models \neg\phi$, afirmación que expresaremos diciendo «ϕ y ψ se contradicen lógicamente».

Definición 1.20.— Sean Φ un conjunto de fórmulas y ϕ una fórmula. Decimos que ψ es *contingente lógicamente* a Φ, precisamente si sucede que ni Φ implica lógicamente a ψ ni Φ contradice lógicamente a ψ; en otras palabras,

$$\psi \text{ es contingente lógicamente a } \Phi \quad \leftrightharpoons \quad \begin{array}{c} \mathcal{M}(\Phi) \subseteq \mathcal{M}(\psi) \\ \wedge \\ \mathcal{M}(\Phi) \cap \mathcal{M}(\psi) \neq \emptyset. \end{array}$$

§ 1.13 Equivalencia lógica

El ser posible hacer para la *replicación lógica* $\phi \mathrel{=\!\!|} \psi$ un estudio similar al hecho para la implicación lógica, nos permite definir la equivalencia lógica en función de ambas.

Definición 1.21.— Decimos que la fórmula ϕ es *lógicamente equivalente* (o, sinónimamente, *tautológicamente equivalente*) a la fórmula ψ, y lo designamos por $\phi \equiv \psi$ (o, sinónimamente, por $\phi \mathrel{=\!\!|\!\models} \psi$)[74], precisamente si $\phi \models \psi$ y $\phi \mathrel{=\!\!|} \psi$ (esto último es, $\psi \models \phi$), es decir, si, y sólo si, para cualquier interpretación $I : \mathcal{V} \longrightarrow \{0, 1\}$, $I(\phi) = I(\psi)$.

La no equivalencia lógica de ϕ y ψ la notamos $\phi \not\equiv \psi$.

[74] Similarmente a lo comentado en la observación 1.10.0 (pág. 146 de esta edición), aunque en algunos textos se usan los símbolos $\equiv$ y $\Leftrightarrow$ indistintamente, reservamos este último para representar el «si, y sólo si,» de nuestro *lenguaje natural*, a diferencia de $\leftrightarrow$, que representa el «si, y sólo si,» de nuestra *lógica ordinaria*. Aún más, en algunos textos se diferencia entre *equivalencia lógica* ($\Leftrightarrow$) y *equivalencia tautológica* ($\equiv$). En una escala de *lenguajes* y *metalenguajes*: $\leftrightarrow$ (nivel 0), $\equiv$ (nivel 1), $\Leftrightarrow$ (nivel 2).

Teorema 1.16
Sean ϕ y ψ fórmulas. Entonces,

$$\phi \equiv \psi \text{ si, y sólo si, } \vDash \phi \leftrightarrow \psi.$$

Ejemplo 101

Si bien aparecen en otros lugares a lo largo de estas notas, recogemos aquí, a modo de una pequeña colección de ejemplos, varias equivalencias lógicas y una no equivalencia lógica. Se satisface:

Principios lógicos:[75]

0. $\phi \equiv \phi$ (Principio de la identidad)
1. $\neg(\phi \land \neg\phi) \equiv \top$; (Principio de la no contradicción)
2. $\phi \lor \neg\phi \equiv \top$; (Principio del tercio excluso)

Algunas leyes de la negación, disyunción y conjunción:

3. $\neg(\phi \land \psi) \equiv \neg\phi \lor \neg\psi$, $\neg(\phi \lor \psi) \equiv \neg\phi \land \neg\psi$; (de De Morgan)
4. $\phi \land \top \equiv \phi$, $\phi \lor \bot \equiv \phi$; (de identidad)
5. $\phi \lor \top \equiv \top$, $\phi \land \bot \equiv \bot$; (de dominación)
6. $\phi \lor \phi \equiv \phi$, $\phi \land \phi \equiv \phi$; (de idempotencia)
7. $\phi \lor \neg\phi \equiv \top$, $\phi \land \neg\phi \equiv \bot$; (de complementación [de negación])
8. $\neg\neg\phi \equiv \phi$; (de involución [de doble negación])
9. $\phi \lor \psi \equiv \psi \lor \phi$, $\phi \land \psi \equiv \psi \land \phi$; (conmutativa)
10. $(\phi \lor \psi) \lor \chi \equiv \phi \lor (\psi \lor \chi)$, $(\phi \land \psi) \land \chi \equiv \phi \land (\psi \land \chi)$; (asociativa)
11. $\phi \lor (\psi \land \chi) \equiv (\phi \lor \psi) \land (\phi \lor \chi)$, $\phi \land (\psi \lor \chi) \equiv (\phi \land \psi) \lor (\phi \land \chi)$; (distributiva)
12. $\phi \lor (\phi \land \psi) \equiv \phi$, $\phi \land (\phi \lor \psi) \equiv \phi$; (de absorción)

Una no equivalencia lógica:

13. $\phi \land \psi \not\equiv \phi \lor \psi$. (por el teorema 1.16 [pág. 157 de esta edición], pues $\phi \land \psi \vDash \phi \lor \psi$, pero $\phi \lor q \nvDash \phi \land \psi$)

Un concepto más débil es el de *$\mathcal{I}$-equivalencia lógica*.

[75] *Vid. supra* § 0.4.4 (p. 39 de esta edición).

Definición 1.22.— Sean ϕ y ψ dos fórmulas y $\mathcal{I}$ un conjunto de interpretaciones. Decimos que ϕ y ψ son *lógicamente $\mathcal{I}$-equivalentes* si, y sólo si, para toda interpretación I de $\mathcal{I}$, $I(\phi) = I(\psi)$. Lo notamos $\phi \equiv_{\mathcal{I}} \psi$.

Ejemplo 102

¿Cuál es el mayor conjunto $\mathcal{I}$ de interpretaciones tal que $\phi \vee \psi$ y $\phi \wedge \psi$ son $\mathcal{I}$-equivalentes?

Resolución.— Se satisface $\phi \vee \psi \equiv_{\{I_{11}, I_{00}\}} \phi \wedge \psi$; en español llano, caso de que ϕ y ψ se satisfagan a la vez o no se satisfaga ninguna, los efectos de su manifestación son indistinguibles: en tal caso, decir 'ϕ o ψ' o decir 'ϕ y ψ', «da igual», afirman lo mismo. ■

Con respecto a la *relación de potencia entre símbolos*, $\vDash$, $\Dashv$ y $\equiv$, al situarse en el metalenguaje (nivel 1), dominan a cualquier juntor (nivel 0). Observemos también que los símbolos $\Rightarrow$ y $\Leftrightarrow$ (que representan el «si ..., entonces ...» [o, sinónimamente, el «...sólo si ...» o el «...implica ...»] y el «...si, y sólo si, ...» del lenguaje natural, respectivamente), pertenecen al nivel 2 del metalenguaje, por lo que dominan a $\vDash$, $\Dashv$ y $\equiv$.

§ 1.14 Teoremas de intercambio y de sustitución

Definición 1.23 (Operación de intercambio).— Sean ψ y ψ^* dos fórmulas y otra fórmula ϕ de la que ψ es subfórmula simple o múltiple. La *operación de intercambio* (o, sinónimamente, *de reemplazo*) consiste en reemplazar una ocurrencia determinada, digamos la primera, de ψ en ϕ por ψ^*.

Las fórmulas ϕ y ϕ^* se denominan *fórmula inicial* y *fórmula final*, respectivamente; las *subfórmulas intercambiadas* ψ y ψ^* se denominan *subfórmula sustituida*, o *reemplazada*, y *subfórmula sustituta*, o *reemplazante*, respectivamente.

Teorema 1.17 (Teorema de intercambio)
Si ψ es una subfórmula de ϕ y reemplazamos ψ en ϕ en una ocurrencia determinada, digamos la primera, por una fórmula lógicamente equivalente ψ^*, entonces, el resultado es una fórmula ϕ^* lógicamente equivalente a ϕ.

Observación 1.14.0.— Cuando estudiemos las reglas de deducción, veremos cómo a la operación de intercambio permite le corresponde una regla del mismo nombre[76], que además refleja lo que establece el teorema de intercambio.

[76] *Cfr. infra* observación 2.2.33 (pág. 213 de esta edición).

Si ψ aparece n veces en ϕ, la aplicación reiterada n veces de la operación de intercambio generará una fórmula final ϕ^* equivalente a la fórmula inicial ψ^*. Este resultado se conoce como teorema de intercambio completo[77].

Teorema 1.18 (Teorema de intercambio completo)
Si ψ es una subfórmula de ϕ y reemplazamos ψ en ϕ, en todas sus ocurrencias, por una fórmula lógicamente equivalente ψ^*, entonces, el resultado es una fórmula ϕ^* lógicamente equivalente a ϕ.

Ejemplo 103

Sea la fórmula $\phi \fallingdotseq (p \wedge q) \to (\neg p \wedge q)$. Consigamos una fórmula equivalente a ϕ que no utilice el juntor $\wedge$.

Resolución.— Sabemos que $p \wedge q \equiv \neg(p|q)$ y por tanto, que $\neg p \wedge q \equiv \neg(\neg p|q)$. Por el teorema de intercambio, aplicado dos veces, $\phi \equiv \neg(p|q) \to \neg(\neg p|q)$. En efecto, utilizando la notación de dicho teorema, lo aplicamos dos veces.

0.ª aplicación del teorema de intercambio.

$$\phi \fallingdotseq (p \wedge q) \to (\neg p \wedge q),$$

$$\psi \fallingdotseq p \wedge q,$$

$$\psi^* \fallingdotseq \neg(p|q),$$

$$\phi^* \fallingdotseq \neg(p|q) \to (\neg p \wedge q);$$

1.ª aplicación del teorema de intercambio.

$$\phi \fallingdotseq \neg(p|q) \to (\neg p \wedge q),$$

$$\psi \fallingdotseq \neg p \wedge q,$$

$$\psi^* \fallingdotseq \neg(\neg p|q),$$

$$\phi^* \fallingdotseq \neg(p|q) \to \neg(\neg p|q).$$



Observación 1.14.1.— En la notación de HOARE, $\phi[\chi/\psi]$ es el resultado de reemplazar todas las ocurrencias de ψ en ϕ por χ (suele leerse «ϕ con χ por ψ»). Notaciones hay muchas[78]. Personalmente, prefiero la notación de ENDERTON [60] (pág. 112), a saber, ϕ^{ψ}_{χ}. De este modo, como muestra,

[77] En algunos textos aparece como *teorema de equivalencia*.
[78] *Vid. v. gr.* https://mathoverflow.net/questions/243084/history-of-the-notation-for-substitution.

el enunciado del teorema de intercambio completo queda:

$$\text{Si } \phi^{\psi} \text{ y } \phi \equiv \psi, \text{ entonces } \phi \equiv \phi^{\psi}_{\psi^*},$$

donde $\phi^{\psi}_{\psi^*}$ es la fórmula final ϕ^* que aparece en el teorema de intercambio.

De ello, igualmente, que hayamos notado por ϕ^{ψ} el hecho de ser ψ una subfórmula de ϕ.

Asimismo, a modo de ejemplo, $\phi^{p,q,r,s}_{0,1,1,0}$ significa que en la fórmula ϕ sustituimos simultáneamente todas las apariciones de p por 0, las de q por 1, las de r por 1 y las de s por 0. Abusando de la notación, cuando no tengamos dudas sobre cuál es la fórmula y cuáles son las variables que sustituimos (y en qué orden las escribimos), nos referiremos a una interpretación de una manera más simple, por ejemplo, I_{0110} (he pues aquí la explicación de lo que hemos venido escribiendo).

Otro resultado interesante es el teorema de sustitución.

Teorema 1.19 (Teorema de sustitución)
Si ϕ es una fórmula válida y ψ es una subfórmula de ϕ y reemplazamos ψ en ϕ en todas sus ocurrencias por una fórmula cualquiera χ, entonces, la fórmula final, ϕ^*, también es una fórmula válida. Con la notación anterior: si $\phi \equiv \top$ y ϕ^{ψ} y ϕ^{ψ}_{χ}, entonces $\phi^{\psi}_{\chi} \equiv \top$.

Observación 1.14.2.— Cuando estudiemos las reglas de deducción (derivación) formal, veremos cómo a la operación de sustitución le corresponde una regla del mismo nombre[79].

Ejemplo 104

Demostremos que $(p \downarrow \neg p) \leftrightarrow \neg(p \vee \neg p)$ es una fórmula válida a partir de saber que $(p \downarrow q) \leftrightarrow \neg(p \vee q)$ es una fórmula válida.

Resolución.— Por el teorema de sustitución, si reemplazamos q por $\neg p$, concluimos que $(p \downarrow \neg p) \leftrightarrow \neg(p \vee \neg p)$ también es una fórmula válida. En efecto, en la notación del teorema 1.19 (pág. 160 de esta edición), hemos aplicado el teorema de sustitución así:

$$\phi \fallingdotseq (p \downarrow q) \leftrightarrow \neg(p \vee q),$$

$$\psi \fallingdotseq q,$$

$$\chi \fallingdotseq \neg p,$$

$$\phi^* \fallingdotseq (p \downarrow \neg p) \leftrightarrow \neg(p \vee \neg p).$$

■

[79] *Cfr. infra* observación 2.2.34 (pág. 213 de esta edición).

Observación 1.14.3.— Para comprobar que dos fórmulas son lógicamente equivalentes pudiésemos usar, entre otros artefactos, éste en línea, SageMath[80]. Por ejemplo, para comprobar que $((p \lor q) \leftrightarrow \top) \land \neg((r \land \neg p) \leftrightarrow \bot) \equiv \neg p \land q \land r$, basta ejecutar el código (el lenguaje es Sage)

```
fórmula = propcalc.formula("(((p|q)<->(tmp|~tmp))␣\&␣~((r&~p)<->(tmp&~tmp)))␣<->␣(~p&q&r)")
fórmula.convert\_cnf\_table()
fórmula
```

Equivalencia funcional entre instrucciones de un lenguaje de programación

Un concepto en cierto grado similar al de equivalencia lógica, coparticipando la noción de sustitución de segmentos válidos de programas (válidos en el sentido de verificados formalmente), es el de *equivalencia funcional* entre instrucciones de un lenguaje de programación; por ejemplo, la sustitución de `sub $0x30,%eax` por `add $-0x30,%eax` en lenguaje ensamblador. Pero, cuidado, hacer esto abre las puertas a la *esteganografía* y a sus variadas estrategias esteganalíticas de ocultación sigilosa de información.

§ 1.15 Base de juntores

Si bien hemos estudiado ya el concepto sintáctico de base de juntores[81], ahora estamos en el ámbito de la semántica. Aquí, interpretaremos algunos de los juntores como *símbolos primitivos* en función de los cuales pueden interpretarse, a su vez, el resto.

Teorema 1.20

Un conjunto de juntores J es una base de juntores precisamente si es posible expresar toda fórmula de $\mathcal{L}_0$ con los juntores de J, esto es, si, y sólo si, es posible expresar todos los demás juntores en función únicamente de los del conjunto J.

Ejemplo 105

Demostremos que el conjunto de los juntores más usuales, $\{\neg, \land, \lor, \rightarrow, \leftrightarrow\}$ es una base de juntores.

Resolución.— Lo es porque los demás juntores pueden expresarse en función de ellos:

$$p \top q \equiv p \lor \neg p \lor q \qquad \equiv 1;$$
$$p \bot q \equiv p \land \neg p \land q \qquad \equiv 0;$$

[80] *Cfr. supra* § 11 (pág. cii de esta edición).
[81] *Vid. supra* § 0.23 (pág. 50 de esta edición).

$$\begin{aligned}
p \operatorname{id}_0 q &\equiv (p \wedge q) \vee (p \wedge \neg q) &&\equiv p\\
p \operatorname{id}_1 q &\equiv (p \wedge q) \vee (\neg p \wedge q) &&\equiv q;\\
p \neg_0 q &\equiv (\neg p \wedge q) \vee (\neg p \wedge \neg q) &&\equiv \neg p;\\
p \neg_1 q &\equiv (p \wedge \neg q) \vee (\neg p \wedge \neg q) &&\equiv \neg q;\\
p \veebar q &\equiv (p \vee q) \wedge \neg(p \wedge q) &&\equiv p \leftrightarrow \neg q \equiv \neg p \leftrightarrow q \equiv \neg(p \leftrightarrow q);\\
p \leftarrow q &\equiv p \vee (\neg p \wedge \neg q) &&\equiv p \vee \neg q \equiv \neg p \to \neg q \equiv q \to p;\\
p \nrightarrow q &\equiv \neg(\neg p \vee q) &&\equiv p \wedge \neg q \equiv \neg(p \to q);\\
p \nleftarrow q &\equiv \neg(p \vee \neg q) &&\equiv \neg p \wedge q \equiv \neg(q \to p);\\
p \mid q &\equiv \neg p \vee \neg q &&\equiv \neg(p \wedge q) \equiv (p \wedge \neg q) \vee \neg p \equiv p \to \neg q;\\
p \downarrow q &\equiv \neg(p \vee q) &&\equiv \neg p \wedge \neg q \equiv \neg(\neg p \to q).
\end{aligned}$$

■

Observación 1.15.0.— En realidad, no debiésemos utilizar la equivalencia lógica ($\equiv$) en estas últimas expresiones, pues lo que hemos hecho es definir «nuevos» juntores a partir de unos dados (de los de la base de juntores). Por ello, quizás mejor utilizar algún signo que exprese dicho acto de definición, por ejemplo, $p \mid q \coloneqq \neg(p \wedge q)$. Sin embargo, son motivos pedagógicos los que me mueven a hacerlo así, pues la realidad es que son equivalencias lógicas y hacerlo de otro modo llevaría seguramente a confusión a quienes tomamos contacto por primera vez con la lógica o la tenemos olvidada en menor o mayor grado.

Ejemplo 106

Demostremos que los conjuntos $\{\neg, \wedge\}$, $\{\neg, \vee\}$ y $\{\neg, \to\}$ son bases de juntores.

Resolución.— En el ejemplo 105 (pág. 161 de esta edición) hemos demostrado que $\{\neg, \wedge, \vee, \to, \leftrightarrow\}$ es una base de juntores. Llamemos Φ_0 a este conjunto. Llamemos a los conjuntos propuestos Φ_1, Φ_2 y Φ_3, respectivamente. Bastará que demostremos que para todo i de 1 a 3, es posible interpretar los juntores de $\Phi_0 \setminus \Phi_i$ como fórmulas basadas únicamente en los juntores de Φ_i.

Y así sucede; en efecto,

$$\begin{aligned}
\{\neg, \wedge\} : p \vee q &\equiv \neg(\neg p \wedge \neg q);\\
p \to q &\equiv \neg(p \wedge \neg q);\\
p \leftrightarrow q &\equiv \neg(p \wedge \neg q) \wedge \neg(\neg p \wedge q).\\
\{\neg, \vee\} : p \wedge q &\equiv \neg(\neg p \vee \neg q);\\
p \to q &\equiv \neg p \vee q;\\
p \leftrightarrow q &\equiv \neg(\neg(\neg p \vee q) \vee \neg(p \vee \neg q)).\\
\{\neg, \to\} : p \wedge q &\equiv \neg(p \to \neg q);
\end{aligned}$$

$$p \vee q \equiv \neg p \rightarrow q;$$
$$p \leftrightarrow q \equiv \neg((p \rightarrow q) \rightarrow \neg(q \rightarrow p)).$$ ■

Ejemplo 107

Demostremos que los conjuntos $\{|\}$ y $\{\downarrow\}$ son bases de juntores.

Resolución.— Por el mismo motivo que en el ejemplo anterior, basta que demostremos que los juntores de $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ pueden representarse en función únicamente de $|$ y $\downarrow$, respectivamente.

En efecto,

		$\{\mid\}$		$\{\downarrow\}$
$\neg p$	$\equiv$	$p \mid p$	$\equiv$	$p \downarrow p$
$p \vee q$	$\equiv$	$(p \mid p) \mid (q \mid q)$	$\equiv$	$(p \downarrow q) \downarrow (p \downarrow q)$
$p \wedge q$	$\equiv$	$(p \mid q) \mid (p \mid q)$	$\equiv$	$(p \downarrow p) \downarrow (q \downarrow q)$
$p \rightarrow q$	$\equiv$	$p \mid (q \mid q)$	$\equiv$	$((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$
$p \leftrightarrow q$	$\equiv$	$(p \mid q) \mid ((p \mid p) \mid (q \mid q))$	$\equiv$	$((p \downarrow p) \downarrow q) \downarrow (p \downarrow (q \downarrow q))$

■

Observación 1.15.1.— En cierto modo, pudiésemos decir que los juntores de la base $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ actúan como «generadores» del resto, de ahí que baste hacerlo para dichos juntores para demostrar que los conjuntos de juntores estudiados en el ejemplo 106 (pág. 162 de esta edición) y en el ejemplo 107 (pág. 163 de esta edición) son bases de juntores.

§ 1.16 Base de juntores minimal

Definición 1.24.— Una *base de juntores minimal* J es una base de juntores en la que ningún juntor de J puede ser definido en función de los demás juntores de J.

Ejemplo 108

Proporcionemos ejemplos de:

0. conjuntos de juntores que no sean bases minimales por no ser bases de juntores;
1. bases de juntores que no sean bases minimales;
2. bases de juntores minimales.

Resolución.— Veamos:

0. los conjuntos $\{\neg\}$, $\{\vee\}$, $\{\wedge\}$, $\{\rightarrow\}$, $\{\leftrightarrow\}$ no son bases minimales, porque ninguno de ellos es una base de juntores;

1. los conjuntos $\{\neg, \vee, \wedge\}$ y $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$, aunque sí son bases de juntores, no son bases minimales;

2. los conjuntos $\{\neg, \wedge\}$, $\{\neg, \vee\}$ y $\{\neg, \rightarrow\}$ son bases de juntores minimales. ■

Teorema 1.21

Las únicas *bases de juntores minimales monádicas* son:

- $\{|\}$,
- $\{\downarrow\}$.

Teorema 1.22

Las únicas *bases de juntores minimales diádicas* son:

- $\{\bot, \rightarrow\}$, $\{\bot, \leftarrow\}$,
- $\{\neg, \vee\}$, $\{\neg, \wedge\}$, $\{\neg, \rightarrow\}$, $\{\neg, \leftarrow\}$, $\{\neg, \nrightarrow\}$, $\{\neg, \nleftarrow\}$,
- $\{\veebar, \rightarrow\}$,
- $\{\rightarrow, \nrightarrow\}$, $\{\rightarrow, \nleftarrow\}$,
- $\{\leftarrow, \veebar\}$, $\{\leftarrow, \nrightarrow\}$, $\{\leftarrow, \nleftarrow\}$,
- $\{\nrightarrow, \leftrightarrow\}$,
- $\{\nleftarrow, \leftrightarrow\}$,
- $\{\top, \nrightarrow\}$, $\{\top, \nleftarrow\}$.

Teorema 1.23

Las únicas *bases de juntores minimales triádicas* son:

- $\{\bot, \vee, \leftrightarrow\}$, $\{\bot, \wedge, \leftrightarrow\}$,
- $\{\vee, \veebar, \leftrightarrow\}$, $\{\vee, \veebar, \top\}$,
- $\{\wedge, \veebar, \leftrightarrow\}$, $\{\wedge, \veebar, \top\}$.

Teorema 1.24

Las únicas bases minimales de juntores son las de los tres teoremas anteriores.

Observación 1.16.0.— En lógica de juntores, trabajar con una base de dos juntores, o incluso de uno, sólo tiene interés teórico, pues haría el cálculo lógico demasiado complejo. Sin embargo, por ejemplo, la importancia de las bases pequeñas es enorme en el análisis y construcción de *circuitos eléctricos*[82].

[82] *Cfr. infra* § 3.6 (pág. 346 de esta edición).

Observación 1.16.1.— En la definición de fórmula[83] pudiésemos sustituir el conjunto J por cualquier base de juntores.

§ 1.17 Lazos entre juntores

Es aceptable ver las definiciones de los juntores en función de los juntores de una base como unas reglas de interdefinición de juntores.

De estas reglas de interdefinición, se destacan clásicamente, las leyes de De Morgan y los principios de Filón y de Crisipo.[84]

Teorema 1.25 (Leyes de De Morgan, I)
Se satisface, para dos variables,

0. $p \wedge q \equiv \neg(\neg p \vee \neg q)$,
1. $p \vee q \equiv \neg(\neg p \wedge \neg q)$,
2. $\neg(p \wedge q) \equiv \neg p \vee \neg q$,
3. $\neg(p \vee q) \equiv \neg p \wedge \neg q$,

Teorema 1.26 (Leyes de De Morgan, II)
Se satisface, para un número finito de variables,

4. $p_0 \wedge p_1 \wedge \ldots \wedge p_n \equiv \neg(\neg p_0 \vee \neg p_1 \vee \ldots \vee \neg p_n)$,
5. $p_0 \vee p_1 \vee \ldots \vee p_n \equiv \neg(\neg p_0 \wedge \neg p_1 \wedge \ldots \wedge \neg p_n)$,
6. $\neg(p_0 \wedge p_1 \wedge \ldots \wedge p_n) \equiv \neg p_0 \vee \neg p_1 \vee \ldots \vee \neg p_n$,
7. $\neg(p_0 \vee p_1 \vee \ldots \vee p_n) \equiv \neg p_0 \wedge \neg p_1 \wedge \ldots \wedge \neg p_n$.

Observación 1.17.0.— Abreviamos:

- $p_0 \wedge p_1 \wedge \ldots \wedge p_n$ por $\bigwedge_{i=0}^{n} p_i$;
- $p_0 \vee p_1 \vee \ldots \vee p_n$ por $\bigvee_{i=0}^{n} p_i$.

[83] *Cfr. supra* definición 0.22 (pág. 49 de esta edición).
[84] Augustus De Morgan (*vid. v. gr.* https://en.wikipedia.org/wiki/Augustus_De_Morgan), Filón de Megara (*vid. v. gr.* https://en.wikipedia.org/wiki/Philo_the_Dialectician) y Crisipo de Solos (*vid. v. gr.* https://en.wikipedia.org/wiki/Chrysippus).

Teorema 1.27 (Principios de FILÓN y de CRISIPO)

Se satisface:

0. Principio de FILÓN: $p \to q \equiv \neg p \vee q$;
1. Principio de CRISIPO: $p \to q \equiv \neg(p \wedge \neg q)$.

El conocido actualmente como principio de FILÓN, este lazo de equivalencia entre la implicación material y la disyunción, es una de las deducciones más famosas de la escuela estoica: el significado de 'si x, entonces y' como 'no x o y'.

Un lazo similar existe entre la equivalencia y la contravalencia.

Teorema 1.28

Se satisface:

0. $p \leftrightarrow q \equiv \neg p \veebar q \equiv p \veebar \neg q$;
1. $p \leftrightarrow q \equiv \neg(p \veebar q)$.

Ejemplo 109

Los gobiernos destinarán un mínimo del 0,7 por ciento de su Producto Interior Bruto (PIB) a programas de cooperación con los pueblos más empobrecidos del planeta, o no lo harán. No hay más posibilidades, ¿verdad?

Resolución.— Procedamos con un análisis lógico elemental. En esencia nos cuestionamos la validez de afirmar «algo ocurre o no ocurre». Validez que puede resultarnos «trivial» desde nuestro sentido común o desde principios «formales» que creamos más elementales, como por ejemplo el principio de FILÓN, a partir del cual se tiene que $p \vee \neg p$ equivale a $\neg p \to \neg p$ —si bien puede que afirmar «si algo ocurre, ocurre» goce para nuestro entendimiento de más crédito que afirmar «algo ocurre o no ocurre»—.

También es posible recurrir a sus tablas de verdad,

p	p	$\boxed{\vee}$	$\neg$	p
1	1	1	0	1
0	0	1	1	0

p	$\neg$	p	$\boxed{\to}$	$\neg$	p
1	0	1	1	0	1
0	1	0	1	1	0

demostrando así, no sólo que $p \vee \neg p$ y $\neg p \to \neg p$ son lógicamente equivalentes, sino además, que ambas son fórmulas válidas, puesto que todas sus interpretaciones,

$$I_0 : \{p\} \to \{0,1\}, \text{ definida por } I_0(p) = 0,$$
$$I_1 : \{p\} \to \{0,1\}, \text{ definida por } I_1(p) = 1,$$

son modelos, tanto para $p \vee \neg p$ como para $\neg p \rightarrow \neg p$.

Si áun quisiésemos decir algo más, observemos que de ahí se tiene $\neg p \vDash \neg p$ (*vid. supra* teorema 1.12 [pág. 147 de esta edición]), lo que expresa y corrobora la propia relación causa-efecto entre un hecho ($\neg p$) y el mismo hecho ($\neg p$), en otras palabras, la reflexividad de $\vDash$ (*vid. supra* teorema 1.15 [pág. 148 de esta edición]). ■

Observación 1.17.1.— En este ejemplo, nos preguntamos por la ley del tercio excluso[85], uno de los principios de la lógica bivalente clásica.

Sin embargo en la realidad puede que no se consiga el 0,7 por ciento pero sí el 0, 66 por ciento o mejor aún, el 0, 77 por ciento, y seguro que nos alegraremos; vamos, que no iremos por ahí diciendo que no lo hemos conseguido, no, seguro que al contrario, celebraremos el éxito.

De hecho, existen otras lógicas en las que no está presente el principio del tercio excluso e incluso éste es rechazado. Pensemos que la realidad cuántica también es diferente: el "gato" está y no está (o tiene un grado de existencia y un grado de inexistencia).

§ 1.18 Deducción semántica

Definición 1.25.— Si conocemos la implicación lógica $\Phi \vDash \psi$ —esto es, si no tenemos que demostrarla porque sabemos que es verdad[86]—, decimos que ψ es *consecuencia lógica inmediata* de Φ (o, sinónimamente, que ψ *se deduce semánticamente de manera inmediata* de Φ).

Ejemplo 110

Demostremos que p es consecuencia lógica inmediata de $\neg\neg p$.

Resolución.— En efecto, si ϕ es $\neg\neg p$ y ψ es p, diremos que ψ es consecuencia lógica inmediata de ϕ, pues existe una equivalencia lógica, que ya conocemos, $\neg\neg p \equiv p$ y, por tanto, una implicación lógica conocida $\neg\neg p \vDash p$, que nos permite deducir semánticamente p a partir de $\neg\neg p$ de manera inmediata. ■

Definición 1.26.— Sean Φ un conjunto de fórmulas y ψ una fórmula. Llamamos *deducción/derivación semántica* (DS) de ψ a partir de Φ, a toda sucesión finita de fórmulas tales que cada una de ellas sea

DS0. una fórmula de Φ, o

DS1. una fórmula válida, o

[85] *Vid. infra* teorema 2.5 (pág. 195 de esta edición).

[86] Desde un punto de vista computacional diríamos que la implicación lógica $\Phi \vDash \psi$ está en una base de conocimiento (*vid. v. gr.* https://en.wikipedia.org/wiki/Knowledge_base) a la que tenemos acceso.

DS2. una fórmula que sea consecuencia lógica inmediata de un subconjunto de fórmulas anteriores en la sucesión.

Observación 1.18.0.— En realidad esto significa que construimos una secuencia de implicaciones lógicas y utilizamos la propiedad transitiva de $\vDash$ para deducir $\phi \vDash \psi$:

$$\text{si } \phi \vDash \phi_0 \text{ y } \phi_0 \vDash \phi_1 \text{ y} \dots \text{y } \phi_n \vDash \psi, \text{ entonces } \phi \vDash \psi.$$

Para hacer las deducciones semánticas, además de las implicaciones y equivalencias lógicas ya estudiadas, utilizamos en anticipación, las reglas deductivas (campo sintáctico) que estudiamos en el capítulo 2 (págs. 176ss. de esta edición) y las reglas semánticas (campo semántico) que estudiamos en el capítulo 3 (págs. 256ss. de esta edición).

Cuando las utilizamos aquí como parte de deducciones semánticas las formulamos como implicaciones o equivalencias lógicas cuya validez, en todo caso, es posible demostrar mediante, por ejemplo, una tabla de verdad.

Esta convivialidad de sintaxis y semántica se debe al hecho de ser la lógica de juntores correcta y completa[87].

Ejemplo 111

«Si echo una mano o soy persona de gran bonhomía, me sentiré satisfecha. Si me siento satisfecha, tendré paz interior. Como no tengo paz interior, esto significa que no eché una mano». ¿Es válida esta argumentación?

[Cubit 23].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si echo una mano o soy persona de gran bonhomía, entonces me siento satisfecha. Si me siento satisfecha, entonces tengo paz interior. No tengo paz interior. Luego, no echo una mano.

1. *Formalización de* $\mathcal{A}$ *en lógica de juntores*.

   - *Variables proposicionales*:

[87] *Cfr. infra* teorema 6.9 (pág. 446 de esta edición).

Considerando como universo de discurso el conjunto de todas las personas, sean las siguientes cuatro variables proposicionales y sus correspondientes significados:

$$p \leftrightharpoons \text{echo una mano},$$
$$q \leftrightharpoons \text{soy persona de gran bonhomía},$$
$$r \leftrightharpoons \text{me siento satisfecha},$$
$$s \leftrightharpoons \text{tengo paz interior}.$$

- *Esquema argumental*:

  Si se supone p o q, se sigue r.
  Si se supone r, se sigue s.
  Se tiene no s.
  ———
  ∴ Se sigue no p.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2\} = \{p \vee q \to r, r \to s, \neg s\}$ y la conclusión ψ, a saber, $\neg p$.

  La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(p \vee q \to r) \wedge (r \to s) \wedge \neg s \to \neg p$. Llamémosla A.

2. *Resolución de* $\mathcal{A}$.

Desde la semántica, se trata de que averigüemos si

$$\{p \vee q \to r, r \to s, \neg s\} \vDash \neg p,$$

esto es, si $\neg p$ es una consecuencia lógica de $\{p \vee q \to r, r \to s, \neg s\}$, tarea que por el teorema 1.14 (pág. 148 de esta edición), equivale a averiguar si

$$\vDash (p \vee q \to r) \wedge (r \to s) \wedge \neg s \to \neg p,$$

es decir, si $(p \vee q \to r) \wedge (r \to s) \wedge \neg s \to \neg p$ es una fórmula válida, para lo que, por ejemplo, tendríamos las siguientes vías.

Vía 0.

Bastaría que hiciésemos su *tabla de verdad*, comprobando que de hecho se trata de una fórmula válida. □

Vía 1.

Otra vía consistiría en utilizar[88] DS0, DS1 y DS2 para construir la siguiente *deducción semántica*.

[88] *Vid. supra* definición 1.26 (pág. 167 de esta edición).

0.	$(p \lor q) \to r$	[DS0] Premisa
1.	$r \to s$	[DS0] Premisa
2.	$\neg s$	[DS0] Premisa
3.	$p \to p \lor q$	[DS1] $\mathrm{ID}_\circ$
4.	$p \to r$	[DS2] Sil 3, 0
5.	$p \to s$	[DS2] Sil 4, 1
6.	$\neg p$	[DS2] MT 5, 2

Observación.— $\mathrm{ID}_\circ$ es la ley *introducción de la disyunción*, $\phi \vDash \phi \lor \psi$; Sil es el *silogismo hipotético*, $(\phi \to \psi) \land (\psi \to \chi) \vDash (\phi \to \chi)$; MT es *modus tollens*, $(\phi \to \psi) \land \neg\psi \vDash \neg\phi$. Todas ellas leyes lógicas que somos capaces de demostrar utilizando tablas de verdad. □

Vía 2.

Una *deducción semántica alternativa*, sin utilizar [DS1], es la siguiente.

0.	$(p \lor q) \to r$	[DS0] Premisa
1.	$r \to s$	[DS0] Premisa
2.	$\neg s$	[DS0] Premisa
3.	$\neg(p \lor q) \lor r$	[DS2] $\mathrm{DI}_\circ$ 0
4.	r	Supuesto
5.	s	[DS2] MP 1, 4
6.	$s \land \neg s$	[DS2] IC 5, 2
7.	$\neg r$	[DS2] RAA 4–6
8.	$\neg(p \lor q)$	[DS2] MT 0, 7
9.	$\neg p \land \neg q$	[DS2] $\mathrm{DM}_\circ$ 8
10.	$\neg p$	[DS2] $\mathrm{EC}_\circ$ 9

Observación.— $\mathrm{DI}_\circ$ es la ley *definición del implicador* (principio de Filón) $\phi \to \psi \mathrel{=\!\!\mid\vDash} \neg\phi \lor \psi$; MP es *modus ponens*, $(\phi \to \psi) \land \phi \vDash \psi$; IC es *introducción del conjuntor*, $\{\phi, \psi\} \vDash \phi \land \psi$; RAA es *reducción al absurdo*, $\phi \to \bot \mathrel{=\!\!\mid\vDash} \neg\phi$; MT es *modus tollens*, $(\phi \to \psi) \land \neg\psi \vDash \neg\phi$; $\mathrm{DM}_\circ$ es De Morgan, $\neg(\phi \lor \psi) \vDash \neg\phi \land \neg\psi$; $\mathrm{EC}_\circ$ es *eliminación del conjuntor*, $\phi \land \psi \vDash \phi$. Todas ellas leyes lógicas demostrables utilizando tablas de verdad.

Para poder obtener $\neg(p \lor q)$ en (8) a partir de (3) necesitamos demostrar que no tenemos r lo cual lo demostramos en el recuadro, suponemos r y llegamos a una fórmula insatisfactible en (6), por lo que, en definitiva, tenemos $\neg r$.

Aunque por motivos pedagógicos hemos optado por hacerlo, lo más usual es no explicitar la utilización de las DS. ■

Observación 1.18.1.— Este estilo con recuadros para supuestos que se cancelan lo usan, por ejemplo, HUTH y RYAN [61].

Observación 1.18.2.— Observemos que hemos demostrado muchísimo más de lo que queríamos. Expresándonos entre lo natural de nuestra lengua y lo artificial del lenguaje lógico, vemos que el caso a estudiar es un «ejemplo», una interpretación, de la argumentación que hemos demostrado. Y por eso precisamente hemos demostrado mucho más, porque hemos demostrado que la argumentación es válida, sea cual sea la interpretación; hemos demostrado que todas las interpretaciones son modelos.

Observación 1.18.3.— La deducción semántica y la *deducción formal*[89] serán revisitadas cuando estudiemos el *sistema de deducción natural*[90].

Observación 1.18.4.— Este ejemplo se complementa con el ejemplo 134 (pág. 223 de esta edición).

§ 1.19 Demostración de ser equivalencia lógica

Una primera vía para demostrar la equivalencia lógica $\phi \equiv \psi$ es:

0.º deducir semánticamente ψ de ϕ, esto es, demostrar $\phi \vDash \psi$, y

1.º deducir semánticamente ϕ de ψ, esto es, demostrar $\phi \dashv \psi$, en definitiva,

$$\phi \vDash \psi \text{ y } \phi \dashv \psi \text{ si, y sólo si, } \phi \equiv \psi.$$

Una segunda vía es construir una secuencia de equivalencias lógicas y utilizar la propiedad transitiva de $\equiv$ para deducirlo:

$$\text{si } \phi \equiv \phi_0 \text{ y } \phi_0 \equiv \phi_1 \text{ y} \ldots \text{y } \phi_n \equiv \psi, \text{ entonces } \phi \equiv \psi.$$

Una tercera, en anticipación, debido a que la lógica de juntores es correcta y completa[91], podremos demostrar una equivalencia lógica demostrando las dos reglas deductivas componentes de la regla deductiva doble correspondiente[92].

[89] *Cfr. infra* § 2.0 (pág. 177 de esta edición).
[90] *Cfr. infra* § 2.2 (pág. 190 de esta edición).
[91] *Vid. infra* teorema 6.9 (pág. 446 de esta edición).
[92] *Vid. infra* § 2.2.1 (pág. 194 de esta edición).

Ejemplo 112

¿Hay una equivalencia lógica en la siguiente afirmación? Si es así, identifiquémosla, formalicémosla y demostrémosla.

> «Que ella no lo hace y él tampoco» se puede decir de una manera algo más complicada, a saber, «que ella lo hace o ella no lo hace pero él sí, no es cierto».

[Cubit 21].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Ella no lo hace y él no lo hace. Luego, es falso que ella lo hace o que ella no lo hace y él sí lo hace. Y recíprocamente.

1. *Formalización en lógica de juntores*.

   - *Variables proposicionales*.

     Considerando como universo de discurso el conjunto de todas las personas, sean las siguientes dos variables proposicionales y sus correspondientes significados:

     $p \risingdotseq$ ella lo hace,

     $q \risingdotseq$ él lo hace.

   - *Esquema argumental*:

$$\frac{\text{Se tiene no } p \text{ y no } q.}{\therefore\ \text{Se sigue no } (p \text{ o } (\text{no } p \text{ y } q)).} \quad \text{y} \quad \frac{\text{Se sigue no } (p \text{ o } (\text{no } p \text{ y } q)).}{\therefore\ \text{Se tiene no } p \text{ y no } q.}$$

   - *Forma lógica*.

     En la equivalencia lógica $\phi \equiv \psi$, identificamos, por una parte, ϕ como la fórmula $\neg p \wedge \neg q$ y ψ como la fórmula $\neg(p \vee (\neg p \wedge q))$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $\neg p \wedge \neg q \leftrightarrow \neg(p \vee (\neg p \wedge q))$. Llamémosla A.

2. *Resolución de $\mathcal{A}$*.

   Si bien pudiésemos resolver $\mathcal{A}$ demostrando que A es una fórmula válida, por ejemplo, mediante una tabla de verdad, vamos a demostrar que, en efecto, $\phi \equiv \psi$ es una equivalencia lógica

mediante encadenamiento transitivo.

$$\begin{aligned}
[0.]\ \neg(p \lor (\neg p \land q)) &\equiv [1.]\ \neg p \land \neg(\neg p \land q) && [\text{De Morgan (negación de } \lor)]\ 0\\
&\equiv [2.]\ \neg p \land (\neg(\neg p) \lor \neg q)) && [\text{De Morgan (negación de } \land)]\ 1\\
&\equiv [3.]\ \neg p \land (p \lor \neg q) && \text{DN } 2\\
&\equiv [4.]\ (\neg p \land p) \lor (\neg p \land \neg q) && [\text{Distributiva de } \land \text{ en } \lor]\ 3\\
&\equiv [5.]\ \text{F} \lor (\neg p \land \neg q) && [\neg p \land p \equiv \text{F}]\ 4\\
&\equiv [6.]\ (\neg p \land \neg q) \lor \text{F} && [\text{Conmutativa de } \lor]\ 5\\
&\equiv [7.]\ \neg p \land \neg q && [\text{Identidad de } \lor]\ 6
\end{aligned}$$ ■

Observación 1.19.0.— La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores, $\neg p \land \neg q \leftrightarrow \neg(p \lor (\neg p \land q))$, no es más que una forma equivalente de la ley de consenso (LCon), a saber, $p \lor (\neg p \land q) \leftrightarrow p \lor q$.[93]

§ 1.20 Notación polaca

Una notación que no usa paréntesis, conocida comúnmente como *notación polaca*, fue desarrollada por Łukasiewicz en 1929. Los juntores se designan por letras mayúsculas en posición prefija: O designa $\bot$, Nα designa $\neg\alpha$, A$\alpha\beta$ designa $\alpha \lor \beta$, K$\alpha\beta$ designa $\alpha \land \beta$, C$\alpha\beta$ designa $\alpha \to \beta$, E$\alpha\beta$ designa $\alpha \leftrightarrow \beta$ y D$\alpha\beta$ designa $\alpha \mid \beta$.

Observación 1.20.0.— El caso de los cuantores en la lógica de primer orden[94] es menos relevante, pues ya de por sí es costumbre situarlos en prefijo; sólo cambian los signos: $\Pi x\alpha$ en vez de $\forall x\alpha$ y $\Sigma x\alpha$ en vez de $\exists x\alpha$.

En definitiva, es cuestión de acostumbrarnos.

Ejemplo 113

Expresemos las reglas de interdefinición $\alpha \land \beta \leftrightarrow \neg(\alpha \to \neg\beta)$, $\alpha \lor \beta \leftrightarrow \neg\alpha \to \beta$ y $(\alpha \leftrightarrow \beta) \leftrightarrow (\alpha \to \beta) \land (\beta \to \alpha)$ en notación polaca.

Resolución.— Aquí están:

$$\begin{aligned}
&\text{K}\alpha\beta \leftrightarrow \text{NC}\alpha\text{N}\beta && \alpha \land \beta \leftrightarrow \neg(\alpha \to \neg\beta),\\
&\text{A}\alpha\beta \leftrightarrow \text{CN}\alpha\beta && \alpha \lor \beta \leftrightarrow \neg\alpha \to \beta,\\
&\text{E}\alpha\beta \leftrightarrow \text{KC}\alpha\beta\text{C}\beta\alpha && (\alpha \leftrightarrow \beta) \leftrightarrow (\alpha \to \beta) \land (\beta \to \alpha);
\end{aligned}$$

como apreciamos, las expresiones son bastante más compactas. ■

[93] *Cfr. infra* observación 2.2.38 (pág. 216 de esta edición).
[94] *Cfr. infra* § 4 (pág. 364 de esta edición).

Además de no usar paréntesis, las ventajas de la notación polaca son muchas; por poner dos ejemplos: 0.º, su escritura se puede realizar en la más simple máquina de escribir, y 1.º, de cara a programar problemas lógicos en un lenguaje para computador, tal como concebimos éstos actualmente, el reconocimiento del juntor más potente es inmediato, pues está situado en la posición cero.

Actividad 1.21

Expresemos los esquemas de fórmulas $\mathrm{KC}\alpha\beta\mathrm{A}\beta\gamma$, $\mathrm{CK}\alpha\beta\mathrm{KN}\beta\gamma$ y $\mathrm{CKCA}\alpha\beta\gamma\mathrm{C}\gamma\mathrm{N}\delta\mathrm{C}\delta\mathrm{N}\beta$ en la base de juntores $\{N, A\}$.

§ 1.21 Bibliografía

- Sobre lógica de juntores:
  - Para una primera aproximación:

[62] María MANZANO ARJONA y Antonia HUERTAS SÁNCHEZ. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

[63] Pascual CASAÑ MUÑOZ y Amador ANTÓN ANTÓN. *Lógica matemática. Ejercicios. I. Lógica de enunciados*. NAU llibres, Valencia, España, 1991.

  - Para estudiar, practicar y conocer más:

[64] Manuel GARRIDO GIMÉNEZ. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

[65] Carmen GARCÍA TREVIJANO. *El arte de la lógica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1999.

  - Para profundizar, acullá:

[66] Manuel GARRIDO GIMÉNEZ, Luis Manuel VALDÉS VILLANUEVA, Jesús MOSTERÍN DE LAS HERAS, Alfonso GARCÍA SUÁREZ y Carlos-Peregrín FERNÁNDEZ OTERO. *Lógica y lenguaje*. Cuadernos de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1989.

[67] Raymond Merrill SMULLYAN. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

[60] Herbert Bruce ENDERTON. *A mathematical introduction to logic*. Harcourt/Academic Press, San Diego, Condado de San Diego, California (US-CA), Estados Unidos de América, 2.ª ed., 2001.

- Sobre lengua española:

[51] Fernando Lázaro Carreter y Vicente Tusón Valls. *Curso de lengua española*. Anaya, Madrid, Comunidad de Madrid (ES-M), España, 1981.

[68] Emilio Alarcos Llorach. *Gramática estructural (según la escuela de Copenhague y con especial atención a la lengua española)*. Biblioteca románica hispánica. Gredos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1984.

[69] Francisco Marcos Marín. *Aproximación a la gramática española*. Colección Didaxis. Cincel, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1975.

 Miguel de Cervantes Saavedra. *El ingenioso hidalgo Don Quijote de la Mancha*.

Cultivemos nuestra lengua

No habrá ser humano completo, es decir, que se conozca y se dé a conocer, sin un grado avanzado de posesión de su lengua. Porque el individuo se posee a sí mismo, se conoce, expresando lo que lleva dentro, y esa expresión sólo se cumple por medio del lenguaje. Hablar es comprender, y comprenderse es construirse a sí mismo y construir el mundo. A medida que se desenvuelve este razonamiento y se advierte esa fuerza extraordinaria del lenguaje en modelar nuestra misma persona, en formarnos, se aprecia la enorme responsabilidad de una sociedad que deja al individuo en estado de incultura lingüística. En realidad, el hombre que no conoce su lengua vive pobremente, vive a medias, aún menos. ¿No nos causa pena, a veces, oír hablar a alguien que pugna, en vano, por dar con las palabras, que al querer explicarse, es decir, expresarse, vivirse, ante nosotros, avanza a trompicones, dándose golpazos, de impropiedad en impropiedad, y sólo entrega al final una deforme semejanza de lo que hubiese querido decirnos? Esa persona sufre como de una rebaja de su dignidad humana. No nos hiere su deficiencia por vanas razones de bien hablar, por ausencia de formas bellas, por torpeza técnica, no. Nos duele mucho más adentro, nos duele en lo humano; porque ese hombre denota con sus tanteos, sus empujones a ciegas por las nieblas de su oscura conciencia de la lengua, que no llega a ser completamente, que no sabremos nosotros encontrarlo. Hay muchos, muchísimos inválidos del habla, hay muchos cojos, mancos, tullidos de la expresión.

(Pedro Salinas Serrano, *El defensor*).

Capítulo 2

Del cálculo de juntores

Del cuero salen las correas.

(Refrán).

De la deducción formal, los sistemas formales y los sistemas deductivos en particular, con especial dedicación a los sistemas de deducción natural, quizás por su aparente cercanía al razonamiento no formal. La afinidad con el álgebra de Boole pudiese servir de excusa al monto de reglas derivadas que se presentan y estudian en este capítulo dedicado al cálculo de juntores.

Dentro del estudio semántico, suele considerarse la diferencia entre *uso* y *mención*. Se dice que se *usa* una palabra o expresión cuando se emplea teniendo presente su significado y que se *menciona* si sólo se la considera como un mero conjunto de símbolos primitivos. Por ejemplo, «gato tiene cuatro patas y gato tiene cuatro letras»; en la primera aparición de la palabra «gato» —justo en este mismo instante estamos mencionando la palabra «gato»°— se está usando, mientras que en la segunda sólo se menciona.

También se diferencia entre *sentido —intensión o connotación—* y *significado —extensión o denotación—*. Por ejemplo, las expresiones «al que madruga, Dios le ayuda» y «*the early bird catches the worm*» tienen el mismo significado; sin embargo, para una persona no muy versada en inglés, la segunda dice «el pájaro tempranero atrapa el gusano», cuyo sentido es distinto a la primera. Por otro lado, si la persona es ducha en inglés, el sentido de ambas también es el mismo.

Si bien al proporcionar un valor a una variable proposicional, por ejemplo, al decir, «p es 'la Tierra es un planeta'» nos preocupamos de interpretar de alguna manera los enunciados lógicos, esto es, del aspecto semántico —aunque en este caso estemos ante una expresión metalingüística—, nos interesa en este momento el análisis *sintáctico*, un mero cálculo de juntores; no obstante, la semántica y la pragmática nos guiarán ineludiblemente en el mismo (somos criaturas humanas, pensantes), mas el tratamiento formal será exclusivamente sintáctico.

§ 2.0 Deducción formal

Definición 2.0.— Sean $\Phi = \{\phi_0, \phi_1, \ldots, \phi_n\}$ un conjunto finito de fórmulas y ψ una fórmula. Una *deducción formal* (o, sinónimamente, *derivación formal*) «de Φ a ψ» es una relación que establece el hecho de ser ψ una «consecuencia formal inmediata» de Φ. Por lo general, llamamos *premisas* a los elementos $\phi_0, \phi_1, \ldots, \phi_n$ de Φ y *conclusión* (*formal*) (*inmediata*) a ψ.

Utilizaremos principalmente el símbolo $\vdash$, metajuntor que llamamos *deductor*, de la siguiente forma:

0. $\Phi \vdash \psi$,
1. $\{\phi_0, \phi_1, \ldots, \phi_n\} \vdash \psi$,
2. $\phi_0, \phi_1, \ldots, \phi_n \vdash \psi$,
3. $\vdash \psi$

que leeremos, respectivamente, por ejemplo,

0. «de Φ se deduce/concluye/sigue (formalmente) (de inmediato/inmediatamente) ψ»,
1. «Φ da lugar (deductiva y formalmente) (de inmediato/inmediatamente) a ψ»,

° La notación entre comillas cuando se menciona una expresión y no se usa, debe su origen a Alfred Tarski.

2. «ψ es consecuencia (deductiva) (formal) (inmediata) de Φ»,

3. ψ es un teorema lógico.

También en algunos textos son usadas las siguientes formalizaciones, en las que se utiliza una partícula del lenguaje natural como «luego», «por consiguiente», «por lo tanto», «así que» o cualquiera de sus sinónimos o un símbolo como el asterismo, $\therefore$», para representar la relación lógica entre las premisas y la conclusión:

$$\begin{array}{rl} & \phi_0 \\ & \phi_1 \\ & \vdots \\ & \phi_n \\ \text{luego} & \psi \end{array} \qquad\qquad \begin{array}{rl} & \phi_0 \\ & \phi_1 \\ & \vdots \\ & \phi_n \\ \therefore & \psi \end{array}$$

En otros textos aparece una raya de separación junto a la partícula o el asterismo:

$$\begin{array}{rl} & \phi_0 \\ & \phi_1 \\ & \vdots \\ & \phi_n \\ \hline \text{luego} & \psi \end{array} \qquad\qquad \begin{array}{rl} & \phi_0 \\ & \phi_1 \\ & \vdots \\ & \phi_n \\ \hline \therefore & \psi \end{array}$$

Y en otros, aparece sólo la raya de separación, con las premisas en disposición vertical u horizontal, lo cual será habitual en la vista de las deducciones formales como reglas de inferencia, que así representadas suelen denominarse *figuras de la deducción* (o, sinónimamente, *esquemas de deducción*) y que denotan una *inferencia inmediata* desde el conjunto de premisas a la conclusión:

$$\begin{array}{c} \phi_0 \\ \phi_1 \\ \vdots \\ \phi_n \\ \hline \psi \end{array} \qquad\qquad \frac{\phi_0 \quad \phi_1 \quad \ldots \quad \phi_n}{\psi}$$

Por eso, también, en otros textos, se explicita el hecho de que la deducción tiene su origen en la conjunción de todas las premisas, si bien desde ese momento sólo hay una premisa, a saber, la proposición compuesta por conjunción:

$$\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \vdash \psi$$

El símbolo $\vdash$ se sitúa en el mismo nivel metalingüístico que los símbolos $\models$ y $\equiv$ (nivel 1), por lo que las consideraciones con respecto a la precedencia o uso de paréntesis son las mismas que las comentadas anteriormente para estos dos, a saber, que domina a cualquier juntor.

En la escala desde el *lenguaje objeto* a los diferentes niveles de *metalenguaje* empleados, se completa lo que comentábamos en la observación 1.10.0 (pág. 146 de esta edición), también en el nivel de metalenguaje correspondiente a la lengua natural[1].

Juntores y metajuntores		Lenguaje y metalenguaje
...sólo si .../ si ..., entonces ...	[$\Rightarrow$]	nivel 3, metalenguaje: lengua natural
...si ...	[$\Leftarrow$]	
...si, y sólo si, ...	[$\Leftrightarrow$]	
de ...se deduce ...	[$\vdash$]	
...se deduce de ...	[$\dashv$]	
...y ...se deducen mutuamente	[$\dashv\vdash$]	
...implica lógicamente ...	[$\models$]	
...es consecuencia lógica de ...	[$=\!\!\mid$]	
...equivale lógicamente a ...	[$\equiv$]	
$\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$		nivel 2, metalenguaje: lenguaje lógico-matemático
$\vdash$, $\dashv$, $\dashv\vdash$, $\models$, $=\!\!\mid$, $\equiv$		nivel 1, metalenguaje: de la lógica de juntores
$\rightarrow$, $\leftarrow$, $\leftrightarrow$		nivel 0, lenguaje objeto: de la lógica de juntores

Cuadro 2.0.— Lenguaje objeto y metalenguaje: juntores, metajuntores y lenguaje natural.

§ 2.0.0 Deducción formal inmediata

Definición 2.1.— Decimos que una fórmula ψ, *se deduce* (o, sinónimamente, *se deriva*) *formalmente de manera inmediata* de un conjunto finito de fórmulas Φ, precisamente si existe la regla deductiva $\Phi \vdash \psi$. En particular, si $\Phi = \{\phi\}$, esto es, si se trata de un conjunto unitario de fórmulas, escribimos $\phi \vdash \psi$ y decimos que ψ se deduce formalmente de manera inmediata de ϕ.

[1] *Cfr. infra* cuadro 2.0 (pág. 179 de esta edición).

Ejemplo 114

¿Es posible afirmar que p se de deduce formalmente de manera inmediata de $\neg\neg p$?

Resolución.— Sí, en efecto, si ϕ es $\neg\neg p$ y ψ es p, es admisible decir que ψ se deduce formalmente de manera inmediata de ϕ, pues existe una regla deductiva, que ya conocemos, $\neg\neg p \vdash p$, que nos permite deducir formalmente p a partir de $\neg\neg p$. ■

§ 2.0.1 Las dos figuras del silogismo hipotético

Como estudiaremos más adelante, una regla deductiva básica[2] del cálculo de juntores (Gentzen, Jaśkowski, 1934) es *modus ponendo ponens* (MPP).

- *Modus ponendo ponens* (MPP) («modo que afirmando, afirma») (o simple y sinónimamente, *modus ponens* (MP)) es la primera figura del *silogismo hipotético* (SH_0); en ella, en la premisa menor se afirma el antecedente y, por tanto, en la conclusión se afirma el consecuente; en formato de regla, «clásico»,

$$\begin{array}{l} \phi \to \psi \\ \underline{\phi \qquad\quad} \\ \psi \end{array}$$

o más «moderno»,

$$\frac{\phi \to \psi \qquad \phi}{\psi}$$

y como ejemplo de regla deductiva derivada[3] del cálculo de juntores, *modus tollendo tollens* (MTT):

- *Modus tollendo tollens* (MTT) («modo que negando, niega»), o simplemente, *modus tollens* (MT), es la segunda figura del *silogismo hipotético* (SH_1); en ella, en la premisa menor se niega el consecuente y, por tanto, en la conclusión se niega el antecedente; en formato de regla, «clásico»,

$$\begin{array}{l} \phi \to \psi \\ \underline{\neg\psi \qquad\quad} \\ \neg\phi \end{array}$$

o más «moderno»,

$$\frac{\phi \to \psi \qquad \neg\psi}{\neg\phi}$$

[2] *Cfr. infra* § 2.2.0 (pág. 190 de esta edición).
[3] *Cfr. infra* § 2.2.1 (pág. 194 de esta edición).

Ejemplo 115

Demostremos que se deducen formalmente de manera inmediata,

0. ψ de $\{\phi \to \psi, \phi\}$;
1. $\neg\phi$ de $\{\phi \to \psi, \neg\psi\}$.

Resolución.— En efecto,

0. por MP, ψ se deduce formalmente de manera inmediata de $\{\phi \to \psi, \phi\}$;
1. por MT, $\neg\phi$ se deduce formalmente de manera inmediata de $\{\phi \to \psi, \neg\psi\}$. ■

§ 2.0.2 Las dos figuras del silogismo contravalente

Son las reglas deductivas derivadas[4] del cálculo de juntores, *modus ponendo tollens* (MPT) y *modus tollendo ponens* (MTP):

- *Modus ponendo tollens* (MPT) («modo que afirmando, niega») es la primera figura del *silogismo contravalente* (SC_0); en ella, en la premisa menor se afirma el antecedente y, por tanto, en la conclusión se niega el consecuente; en formato de regla, «clásico»,

$$\begin{array}{l} \phi \veebar \psi \\ \phi \\ \hline \neg\psi \end{array}$$

o más «moderno»,

$$\frac{\phi \veebar \psi \qquad \phi}{\neg\psi}$$

- *Modus tollendo ponens* (MTP) («modo que negando, afirma») es la segunda figura del *silogismo contravalente* (SC_1) y la única figura del *silogismo disyuntivo* (SD); en ella, en la premisa menor se niega el antecedente y, por tanto, en la conclusión se afirma el consecuente; en formato de regla, «clásico»,

$$\begin{array}{l} \phi \veebar \psi \\ \neg\phi \\ \hline \psi \end{array} \qquad\qquad \begin{array}{l} \phi \vee \psi \\ \neg\phi \\ \hline \psi \end{array}$$

o más «moderno»,

$$\frac{\phi \veebar \psi \qquad \neg\phi}{\psi} \qquad\qquad \frac{\phi \vee \psi \qquad \neg\phi}{\psi}$$

[4] *Cfr. infra* § 2.2.1 (pág. 194 de esta edición).

Ejemplo 116

Demostremos que se deducen formalmente de manera inmediata,

0. ψ de $\{\phi \vee \psi, \neg\phi\}$;
1. $\neg\psi$ de $\{\phi \veebar \psi, \phi\}$.

Resolución.— En efecto,

0. por MTP, ψ se deduce formalmente de manera inmediata de $\{\phi \vee \psi, \neg\phi\}$;
1. por MPT, $\neg\psi$ se deduce formalmente de manera inmediata de $\{\phi \veebar \psi, \phi\}$ (y alternativamente de $\{\neg(\phi \leftrightarrow \psi), \phi\}$, pues $\neg(\phi \leftrightarrow \psi) \dashv\vdash \phi \veebar \psi$). ■

Observación 2.0.0.— Notaremos la acción de estas reglas funcionalmente con sus acrónimos, por ejemplo, la acción de *modus ponendo tollens* sobre dos fórmulas ϕ y ψ por MPT(ϕ, ψ) o MPT(t_0, t_1) si dichas fórmulas están designadas por las etiquetas t_0 y t_1, respectivamente (alternativamente, con $\{\}$ en vez de paréntesis).

§ 2.0.3 Deducción formal

Definición 2.2.— Sean Φ un conjunto de fórmulas y ϕ una fórmula. Denominamos *deducción* (o, sinónimamente, *derivación*) *formal* de ϕ a partir de Φ, a toda sucesión finita de fórmulas, tales que cada una de ellas sea:

DF0. una fórmula de Φ, o

DF1. un teorema lógico, o

DF2. una fórmula que se deduzca/derive inmediatamente de un subconjunto de fórmulas anteriores en la sucesión.

Observación 2.0.1.— En realidad esto significa que construimos una secuencia de deducciones formales y utilizamos la propiedad transitiva de $\vdash$ para deducir $\phi \vdash \psi$:

$$\text{si } \phi \vdash \phi_0 \text{ y } \phi_0 \vdash \phi_1 \text{ y} \ldots \text{y } \phi_n \vdash \psi, \text{ entonces } \phi \vdash \psi.$$

Ejemplo 117

Demostremos que $\neg p$ se deriva formalmente de $\{p \to q, \neg q\}$.

Resolución.— En el ejemplo 115 (pág. 181 de esta edición) ya demostramos que $\neg p$ se deduce formalmente de manera inmediata de $\Phi = \{p \to q, \neg q\}$; pues bien, es posible demostrar también que $\neg p$ se *deduce formalmente* de $\{p \to q, \neg q\}$, y esto es precisamente porque puede aplicarse *modus tollendo tollens* (MT). En efecto,

0.	$p \to q$	[DF0] Premisa
1.	$\neg q$	[DF0] Premisa
2.	$\neg p$	[DF2] MT 0, 1



Ejemplo 118

Sirva como tal el ejemplo 134 (pág. 223 de esta edición).

Teorema 2.0

Toda regla de inferencia deductiva es una deducción formal.

Pero aún más, la deducción formal es un procedimiento que proporciona nuevas reglas de inferencia deductivas —*reglas derivadas*—. Por esto no presenta inconsistencia que designemos, como además es habitual, por $\Phi \vdash \phi$ el hecho de que ϕ se deduzca formalmente de Φ, esto es, de que ϕ sea el último término de una deducción formal desde Φ.

El algoritmo de inferencia hacia adelante

En el trabajo con una *base de conocimiento* (veámosla como un conjunto de fórmulas) se utiliza el conocido como *algoritmo de inferencia hacia delante*: a partir de un conjunto R de reglas de inferencia, es decir, del tipo $\{\phi_0, \phi_1, \ldots, \phi_k\} \vdash \psi$, este algoritmo recorre todas las posibles premisas (subconjuntos de fórmulas de la base de conocimiento) y cada vez que exista una regla de R cuyo conjunto de premisas sea uno de tales subconjuntos, añade la conclusión a la base de conocimiento. Este proceso se repite hasta que no se puedan hacer más adiciones a la base de conocimiento.

En este ámbito, dada una base de conocimientos Φ y un conjunto de reglas R, decimos que *de Φ se deriva ϕ con las reglas R* si ϕ está en Φ o si ϕ es añadida a Φ durante la ejecución del algoritmo de inferencia hacia adelante utilizando el conjunto de reglas R.

Confusiones (LEÓN ROJAS [1], pág. 7)

Cuatro operadores aparecen con frecuencia en los razonamientos lógicos: *modus ponendo ponens* ($A \to B \wedge A \vdash B$), *modus tollendo tollens* ($A \to B \wedge \neg B \vdash \neg A$), la *ley del silogismo* ($A \to B \wedge B \to C \vdash A \to C$) y la *ley de los contrapuestos* ($A \to B \vdash \neg B \to \neg A$). No es raro saber que el ser humano los confunde, como también confunde *validez* y *verdad*. Es típica, por ejemplo, la confusión de *modus tollendo tollens* con la ley de los contrapuestos, a partir de apreciar únicamente la verdad de q, cuando se considera la validez de $p \to q$ (*cfr.* WASON y JOHNSON-LAIRD [70]; REVLIN, LEIRER, YOPP y YOPP [71]; NICKERSON, PERKINS y SMITH [72]).

Más aún. Bruno LATOUR [73] (pág. 189) relata la experiencia de comprensión de razonamientos sencillos que realizó Alexander Romanovich LURIA [74] entre personas campesinas de la antigua Unión Soviética. Por ejemplo: «En el polo norte todos los osos son blancos; Novaya Zemyla está en el polo norte. ¿De qué color son allí los osos? —No lo sé. Deberías preguntarle a la gente que ha viajado por allí y los han visto». Aparentemente, estas personas campesinas no son capaces de aplicar *modus ponendo ponens*. De esta experiencia, uno pudiese inferir que no son nada lógicas, pues no aplican el operador adecuado. Sin embargo, Michael COLE y Sylvia SCRIBNER [75] hicieron un experimento similar en Liberia, donde a las personas campestres que decían esto, se les pedía explicar su razonamiento, diciendo que para conocer el color de algo, tenían que verlo, y que para ver algo, tenían que estar junto a ese algo. Como ellas no estaban en el polo norte y no podían ver los osos, no eran capaces de responder a la cuestión. ¡Pues anda si son lógicas! Su razonamiento es un ejemplo de aplicación de *modus tollendo tollens*.

§ 2.1 Sistemas deductivos

Definición 2.3.— Un *sistema deductivo* $\mathcal{D}$ está formado por dos conjuntos:

0. un conjunto Λ, vacío, finito o infinito numerable, de fórmulas, denominadas *axiomas* de $\mathcal{D}$, y
1. un conjunto $\mathcal{R}$, no vacío, de *reglas de inferencia deductivas*.

Grosso modo, se distinguen dos tipos de sistemas deductivos, los *sistemas axiomáticos* («tipo HILBERT»), si Λ no es vacío y los *sistemas de deducción natural* («tipo GENTZEN-JAŚKOWSKI»), si Λ es vacío.

Los sistemas formales axiomáticos de la lógica de juntores se desarrollaron fundamentalmente en el siglo XX, por ejemplo, el sistema PM de RUSSELL y WITHEHEAD [76] (1910), el sistema de HILBERT y ACKERMANN [77] (1928), el sistema L de ŁUKASIEWICZ [78] (1929) o el sistema K de KLEENE [79] (1952). En esta edición de estas notas no estudiamos ninguno de éstos. Sin embargo, sí que dedicaremos un capítulo a la axiomática de conjuntos (*cfr. infra* capítulo 14 [págs. 752ss. de esta edición]).

Sí que estudiamos el sistema de deducción natural de GENTZEN [80] (1935) y JAŚKOWSKI [81] (1934) (elaborado de manera independiente por ambos).

Observación 2.1.0.— Los sistemas de deducción natural se denominan así porque en ellos las deducciones imitan, de alguna manera, la deducción intuitiva que posee cualquier ser humano. En este sentido son más «naturales» que los sistemas axiomáticos. Básicamente, la diferencia entre un sistema formal axiomático y un sistema formal de deducción natural radica en que en el primero se presupone la validez de uno o varios axiomas mientras que ninguno en el segundo. Por ejemplo, pensemos en el juego de ajedrez: un sistema tipo GENTZEN-JAŚKOWSKI puede actuar en cualquier momento de una partida, siendo cualquier posicionamiento de las fichas —i.e. un axioma— externa al sistema. Para que un sistema axiomático pudiese actuar igual, debería incluir todos los posicionamientos posibles —axiomas—.

Observación 2.1.1.— Si bien hemos definido un sistema de deducción natural si Λ es vacío, en algunos textos aparece la regla de inferencia deductiva Identidad[5], $A \vdash A$, de un sistema de deducción natural interpretada como un axioma, aunque siguen considerando dicho sistema como no axiomático.

Ejemplo 119 (El sistema formal MIU)

El *sistema formal MIU*, un sistema deductivo propuesto por HOFSTADTER [2], se define como sigue.

$\Sigma = \{M, I, U\}$ (alfabeto de MIU) [las únicas letras con las que formar palabras],

$\Lambda = \{MI\}$ (axioma de MIU) [la palabra MI, la única conocida al comienzo],

$\mathcal{R} = \{R_{\text{I}}, R_{\text{II}}, R_{\text{III}}, R_{\text{IV}}\}$ (reglas de inferencia), donde estas reglas son:

Regla I: si xI es un teorema, también lo es xIU.

Regla II: si Mx es un teorema, también lo es Mxx.

Regla III: puede reemplazarse III por U en cualquier teorema.

Regla IV: puede suprimirse UU de cualquier teorema.

En formato de reglas, dadas cualesquiera dos fórmulas α y β,

$$R_{\text{I}} : \frac{\alpha I}{\alpha IU} \quad R_{\text{II}} : \frac{M\alpha}{M\alpha\alpha} \quad R_{\text{III}} : \frac{\alpha III\beta}{\alpha U\beta} \quad R_{\text{IV}} : \frac{\alpha UU\beta}{\alpha\beta}.$$

Definición 2.4.— Sea Φ un conjunto de fórmulas. Llamamos *teorema* de Φ en $\mathcal{D}$ a cualquier fórmula ϕ que sea deducible formalmente de $\Lambda \cup \Phi$ mediante las reglas de inferencia de $\mathcal{R}$. Notamos $\Phi \vdash_{\mathcal{D}} \phi$

[5] *Vid. infra* teorema 2.8 (pág. 198 de esta edición).

o simplemente $\Phi \vdash \phi$ si no ha lugar a confusión. A las fórmulas de $\Lambda \cup \Phi$ las llamamos *premisas* o *hipótesis* del teorema; ϕ es la *conclusión* o *tesis*.

Si todas las premisas son axiomas, es decir, si $\Phi \subseteq \Lambda$, entonces $\Phi \vdash \phi$ no es más que $\emptyset \vdash \phi$. Esto suele notarse $\vdash \phi$ y denominarse *teorema lógico* (en el sistema deductivo $\mathcal{D}$).

Ejemplo 120

Preguntémonos ahora si

$$\vdash_{MIU} MUIUI$$

esto es, si $MUIUI$ es un teorema lógico en MIU.

[Cubit 129].

Resolución.— Observemos que al preguntarnos si es un teorema lógico, estamos considerando que $\Phi = \emptyset$, es decir, que la única premisa es el axioma MI.

Vemos que efectivamente sí es cierto que $\vdash_{MIU} MUIUI$. Para ello, vemos que $MUIUI$ es deducible formalmente de Λ mediante las reglas de inferencia de $\mathcal{R}$. En efecto,

0.	MI	[axioma]
1.	MII	[0 y R_{II}]
2.	$MIIII$	[1 y R_{II}]
3.	MUI	[2 y R_{III}]
4.	$MUIUI$	[3 y R_{II}]



Este ha sido un ejemplo de cómo demostrar que una fórmula es un teorema MIU. Veamos a continuación un ejemplo de una fórmula que no es un teorema MIU.

Ejemplo 121

El rompecabezas MU.

¿Es MU un teorema del sistema MIU?, esto es, ¿es posible generar la palabra MU en el sistema MIU? La respuesta es que no, que MU no es un teorema MIU.

[Cubit 130].

Resolución.— Tras una inspección atenta es fácil conjeturar un par de cosas sobre los teoremas del sistema MIU.

Intuición 0: Todos los teoremas comienzan con M;

Intuición 1: No hay manera de eliminar I; en otras palabras, el número de veces que aparece I en cualquier fórmula es no nulo.

Llamemos $\mathrm{N}[I]$ al número de veces que aparece I en una fórmula dada —N es el *contador*, un *cuantor aritmético* elemental[6]—. Si MU fuese un teorema MIU, entonces en algún estado de la derivación formal, $\mathrm{N}[I] = 0$. Por contraposición, si demostramos que $\mathrm{N}[I]$ no puede ser cero en ningún estado, habremos demostrado que MU no es un teorema MIU.

¿Qué sabemos?

Conocimiento 0: $\mathrm{N}[I]_0$, el valor inicial de $\mathrm{N}[I]$, es 1 (ya que el único axioma MIU es MI);

Conocimiento 1: R_{I} y R_{IV} no afectan a $\mathrm{N}[I]$;

Conocimiento 2: R_{III} decrementa $\mathrm{N}[I]$ en 3;

Conocimiento 3: R_{II} duplica $\mathrm{N}[I]$.

Pues bien, tras aplicar p veces la regla R_{II} y q veces la regla R_{III}, el $\mathrm{N}[I]$ correspondiente a la fórmula producida vale $(2^p - 3q) \cdot \mathrm{N}[I]_0$, que como $\mathrm{N}[I]_0 = 1$, queda

$$2^p - 3q = 0; \tag{2.0}$$

es decir, que $\mathrm{N}[I]$ sea 0 en algún estado de la derivación, equivale a que existan $p, q \in \mathbb{Z}^+$, tales que $2^p - 3q = 0$, lo que no es posible, ¿verdad?

Debemos así demostrar que $\forall p, q \in \mathbb{Z}^+, 2^p \neq 3q$, cuestión que demostraremos en el ejemplo 413 (pág. 807 de esta edición). ■

Observación 2.1.2.— Pensemos en que en realidad hemos demostrado que en ningún estado de la derivación/computación, $N[I]$ es múltiplo de 3.

Actividad 2.0

El rompecabezas *MI*.— Pudiésemos plantear el rompecabezas MI, en cierto sentido «dual» y «equivalente» al rompecabezas MU. Para ello, construimos el sistema UIM, con el mismo alfabeto anterior, el único axioma, MU, y como reglas, las recíprocas de las anteriores —por ejemplo, la UIM-Regla I: si xIU es un teorema, también lo es xI—. El rompecabezas MI es: ¿Es MI un teorema UIM?

[6] En el ámbito de la computación práctica, un *contador* es una variable numérica cuyo valor se incrementa o decrementa con cantidades fijas (por ejemplo, i cuenta al final el número de iteraciones del bucle: $i \leftarrow 0$; mientras $i < 100$; $i \leftarrow i + 1$; fin mientras;); un *acumulador*, por otra parte, es una variable numérica cuyo valor se incrementa o decrementa con cantidades variables (por ejemplo, s acumula al final la suma de los cien primeros números enteros positivos: $i \leftarrow 0$; $s \leftarrow 0$; mientras $i < 100$; $i \leftarrow i + 1$; $s \leftarrow s + i$; fin mientras;).

Actividad 2.1

Expresemos la regla: para sumar tres números, sumemos el tercero a la suma de los dos primeros.

Con miras a su resolución.— Una expresión lógico-matemática de esta regla es:

$$\frac{\begin{array}{l} r \hookleftarrow x + y \\ s \hookleftarrow r + z \end{array}}{s \hookleftarrow (x + y) + z}$$

Teorema 2.1

Sean $\mathcal{D}$ un sistema deductivo, Φ un conjunto de fórmulas y T el conjunto de todos los teoremas de Φ en $\mathcal{D}$. Entonces:

0. $\Lambda \cup \Phi \subseteq T$.
1. T es cerrado para todas y cada una de las reglas de inferencia, básicas y derivadas.
2. T es el menor, en el sentido de la inclusión, de todos los conjuntos de fórmulas que satisfacen (0) y (1) —en realidad, es la intersección de todos ellos—.
3. *Principio de Inducción para Teoremas* (PIT): Si $S \subseteq T$ y S satisface (0) y (1), entonces $S = T$.

Teorema 2.2 (Propiedades)

Sean ϕ y ψ fórmulas y Φ y Ψ conjuntos de fórmulas. Se satisfacen las siguientes propiedades:

0. si $\Phi \subseteq \Psi$ y $\Phi \vdash \phi$, entonces $\Psi \vdash \phi$; (monotonía)
1. $\Phi \vdash \phi$ si, y sólo si, existe $\Phi_0 \subseteq \Phi$, Φ_0 finito, tal que $\Phi_0 \vdash \phi$; (compacidad)
2. si $\Phi \vdash \phi$ y para toda fórmula ψ de Φ, $\Psi \vdash \psi$, entonces $\Psi \vdash \phi$. (transitiva —regla T—)

Teorema 2.3 (Teorema de la deducción (TD))

Sean Φ un conjunto de fórmulas y ϕ y ψ fórmulas; entonces

$$\text{si } \Phi \cup \{\phi\} \vdash \psi, \text{ entonces } \Phi \vdash \phi \to \psi.$$

Teorema 2.4 (Teorema recíproco del teorema de la deducción (TRD))

Sean Φ un conjunto de fórmulas y ϕ y ψ fórmulas; entonces

$$\text{si } \Phi \vdash \phi \to \psi, \text{ entonces } \Phi \cup \{\phi\} \vdash \psi.$$

Ejemplo 122

Demostremos que se satisface

$$\phi_0, \phi_1, \ldots, \phi_n \vdash \phi \text{ si, y sólo si, } \phi_0, \phi_1, \ldots, \phi_{n-1} \vdash \phi_n \to \phi.$$

Resolución.— En efecto, se satisface la doble implicación:

→) por el teorema de la deducción (TD) aplicado a $\Phi \leftrightharpoons \{\phi_0, \phi_1, \ldots, \phi_{n-1}\}$, $\phi \leftrightharpoons \phi_n$ y $\psi \leftrightharpoons \phi$;

←) por el teorema recíproco (TRD) aplicado a las anteriores Φ, ϕ y ψ. ■

Observación 2.1.3.— Si $\Phi = \emptyset$, TD y TRD establecen que afirmar que de ϕ se deduce formalmente ψ equivale a afirmar que $\phi \to \psi$ es un teorema lógico:

$$\phi \vdash \psi \Leftrightarrow \vdash \phi \to \psi \tag{2.1}$$

En particular, afirmar $\phi \vdash \phi$, esto es, afirmar que ϕ se deduce de ϕ, equivale a afirmar el teorema lógico $\vdash \phi \to \phi$.

Jesús Mosterín [82] (pág. 88) llama primer teorema de la deducción a (2.1).

La acción conjunta de TD y TRD permite entonces reescribir la regla de deducción

$$\phi_0, \phi_1, \ldots, \phi_n \vdash \phi,$$

como el teorema lógico

$$\vdash (\phi_0 \land \phi_1 \land \ldots \land \phi_n) \to \phi,$$

esto es,

$$\frac{\phi_0 \quad \phi_1 \quad \ldots \quad \phi_n}{\phi} \quad \text{si, y sólo si,} \quad \frac{}{(\phi_0 \land \phi_1 \land \ldots \land \phi_n) \to \phi}.$$

Una proyección a la lógica de juntores es

$$((\phi_0 \land \phi_1 \land \ldots \phi_n) \to \phi) \leftrightarrow (\phi_0 \to (\phi_1 \to (\ldots \to \phi_n) \ldots),$$

por ejemplo, si $n = 4$,

$$((\phi_0 \land \phi_1 \land \phi_2 \land \phi_3 \land \phi_4) \to \phi) \leftrightarrow (\phi_0 \to (\phi_1 \to (\phi_2 \to (\phi_3 \to \phi_4)))).$$

Definición 2.5.— Llamamos *teoría formal* a un sistema deductivo más un conjunto de fórmulas no axiomas.

Ejemplo 123

El sistema deductivo MIU más, por ejemplo, el conjunto de fórmulas —teoremas lógicos— $\{MII, MUI, MUIUI\}$ es una teoría formal.

Observación 2.1.4.— Ya que de nuevo toma protagonismo, notemos que no conocemos todos los teoremas lógicos en *MIU*, pero que esto no nos extrañe, es de lo más normal, ¿verdad?; ¿quién conoce, si no, exhaustivamente, todos los teoremas de alguna teoría matemática al uso?

§ 2.2 Sistema de Deducción Natural (SDN)

La presente exposición se fundamenta en el *sistema de deducción natural*, elaborado independientemente por Gentzen [80] (1935) y Jaśkowski [81] (1934). En él, a partir de unas reglas básicas de inferencia, es posible resolver cualquier problema deductivo.

§ 2.2.0 Reglas deductivas básicas

Vemos a continuación las *reglas de inferencia deductivas básicas* del SDN.

Regla de introducción del implicador (II)

Esta regla es justamente el *teorema de la deducción* (TD) (*cfr. supra* teorema 2.3 [pág. 188 de esta edición]). Su esquema argumental es

$$\begin{array}{ll} & \text{Si se supone } \phi\text{, se sigue } \psi. \\ \hline \therefore & \text{Se sigue que } \phi \to \psi. \end{array}$$

Diferentes formas de escribir la regla de deducción correspondiente son:

$$\{\phi \vdash \psi\} \vdash (\phi \to \psi) \qquad \frac{\phi \vdash \psi}{\phi \to \psi} \qquad \begin{array}{|l} \phi \\ \vdots \\ \psi \\ \hline \end{array} \atop \phi \to \psi$$

Observación 2.2.0.— Notemos la diferencia con lo que correspondería al esquema argumental

$$\begin{array}{ll} & \text{Se tiene que } \phi \to \psi. \\ \hline \therefore & \text{Se sigue que } \phi \to \psi. \end{array}$$

cuya regla de deducción correspondiente es la identidad (Id), es decir,

$$\frac{\phi}{\phi}$$

que reescrita en los términos de $\phi \to \psi$, en las formas anteriores, es:

$$\{\phi \rightarrow \psi\} \vdash (\phi \rightarrow \psi) \qquad \frac{\phi \rightarrow \psi}{\phi \rightarrow \psi} \qquad \frac{\phi \rightarrow \psi}{\phi \rightarrow \psi}$$

Regla de eliminación del implicador (EI)

Esta regla es justamente *modus ponendo ponens* (MPP) —«modo que afirmando, afirma», a veces referido simplemente por *modus ponens* (MP)—. Ya hemos comentado (*cfr. supra* ejemplo 115 [pág. 181 de esta edición]) que tradicionalmente es una figura del llamado silogismo hipotético (SH_o). También se la conoce como *regla o principio de separación* en referencia a que el consecuente se separa. Su esquema argumental es

Se tiene que $\phi \rightarrow \psi$.
Se tiene ϕ.

$\therefore$ Se sigue ψ.

Diferentes formas de escribir la regla de deducción correspondiente son:

$$\{\phi \rightarrow \psi, \phi\} \vdash \psi \qquad \frac{\phi \rightarrow \psi \qquad \phi}{\psi} \qquad \frac{\begin{array}{l}\phi \rightarrow \psi\\ \phi\end{array}}{\psi}$$

Regla de introducción del conjuntor (IC)

También se la conoce como *ley del producto* (Prod). Su esquema argumental es

Se tiene ϕ.
Se tiene ψ.

$\therefore$ Se sigue $\phi \wedge \psi$.

Diferentes formas de escribir la regla de deducción correspondiente son:

$$\{\phi, \psi\} \vdash \phi \wedge \psi \qquad \frac{\phi \qquad \psi}{\phi \wedge \psi} \qquad \frac{\begin{array}{l}\phi\\ \psi\end{array}}{\phi \wedge \psi}$$

Regla de eliminación del conjuntor (EC)

También se la conoce como *regla de simplificación* (Simp) o *ley de Pedro* HISPANO. Dos modalidades según el consecuente sea ϕ o ψ, siendo sus esquemas argumentales respectivos:

Se tiene $\phi \wedge \psi$.

$\therefore$ Se sigue ϕ.

Se tiene $\phi \wedge \psi$.

$\therefore$ Se sigue ψ.

Diferentes formas de escribir las reglas de deducción correspondientes a ambas modalidades son:

EC_0:

$$\{\phi \wedge \psi\} \vdash \phi \qquad \frac{\phi \wedge \psi}{\phi}$$

EC_1:

$$\{\phi \wedge \psi\} \vdash \psi \qquad \frac{\phi \wedge \psi}{\psi}$$

Regla de introducción del disyuntor (ID)]

También llamada *ley de adición* (Ad) o *ley de ampliación disyuntiva*. Dos modalidades según el antecedente sea ϕ o ψ, siendo sus esquemas argumentales respectivos:

	Se tiene ϕ.
∴	Se sigue $\phi \vee \psi$.

	Se tiene ψ.
∴	Se sigue $\phi \vee \psi$.

Diferentes formas de escribir las reglas de deducción correspondientes a ambas modalidades son:

ID_0:

$$\{\phi\} \vdash \phi \vee \psi \qquad \frac{\phi}{\phi \vee \psi}$$

ID_1:

$$\{\psi\} \vdash \phi \vee \psi \qquad \frac{\psi}{\phi \vee \psi}$$

Regla de eliminación del disyuntor (ED)

También llamada *prueba por casos* (Cas). El esquema argumental es:

	Se tiene $\phi \vee \psi$.
	Si se supone ϕ, se sigue χ.
	Si se supone ψ, se sigue χ.
∴	Se sigue χ.

Diferentes formas de escribir la regla de deducción correspondiente son:

$$\{\phi \vee \psi, \phi \vdash \chi, \psi \vdash \chi\} \vdash \chi$$

$$\frac{\phi \vee \psi \qquad \phi \vdash \chi \qquad \psi \vdash \chi}{\chi}$$

$$\frac{\phi \vee \psi \quad \left|\begin{array}{l}\phi\\ \vdots\\ \chi\end{array}\right. \quad \left|\begin{array}{l}\psi\\ \vdots\\ \chi\end{array}\right.}{\chi}$$

$$\begin{array}{l}\phi \vee \psi\\ \left|\begin{array}{l}\phi\\ \vdots\\ \chi\end{array}\right.\\ \left|\begin{array}{l}\psi\\ \vdots\\ \chi\end{array}\right.\\ \hline \chi\end{array}$$

Regla de introducción del negador (IN)

Dos apuntes: 0.º, en esta regla se hace uso de una *subderivación* (bajo la hipótesis adicional ϕ, hemos concluido ψ —subderivación de ψ a partir de ϕ—), y 1.º, esta regla formaliza la *demostración por reducción al absurdo* (Abs, RAA): si de la hipótesis adicional ϕ, se sigue una fórmula insatisfactible $(\psi \wedge \neg\psi)$, entonces se concluye $\neg\phi$.

El esquema argumental es

$$\begin{array}{ll} & \text{Si se supone } \phi\text{, se sigue } \psi \wedge \neg\psi. \\ \hline \therefore & \text{Se sigue } \neg\phi. \end{array}$$

Diferentes formas de escribir la regla de deducción correspondiente son:

$$\{\phi \vdash (\psi \wedge \neg\psi)\} \vdash \neg\phi \qquad \frac{\phi \vdash (\psi \wedge \neg\psi)}{\neg\phi} \qquad \frac{\left|\begin{array}{l}\phi\\ \vdots \\ \psi \wedge \neg\psi\end{array}\right.}{\neg\phi}$$

Regla de eliminación del negador (EN)

Suele conocerse también como *regla de doble negación* (DN). El esquema argumental es

$$\begin{array}{ll} & \text{Se tiene } \neg\neg\phi. \\ \hline \therefore & \text{Se sigue } \phi. \end{array}$$

Diferentes formas de escribir la regla de deducción correspondiente son:

$$\{\neg\neg\phi\} \vdash \phi \qquad \frac{\neg\neg\phi}{\phi}$$

Observación 2.2.1.— Ocho reglas: introducción y eliminación del implicador, conjuntor, disyuntor y negador: II, EI, IC, EC, ID, ED, IN y EN.

Observación 2.2.2.— El apartado 2 del ejemplo 153 (pág. 273 de esta edición), proporciona una formulación alternativa del sistema de deducción natural, a saber, si admitimos DU2 y las reglas básicas de eliminación de $\wedge$, sobran las de introducción de $\vee$.

Observación 2.2.3.— De aquí en adelante, nos tomamos la licencia de expresar $\{\phi_0, \phi_1, \ldots, \phi_n\} \vdash \psi$ simplemente por $\phi_0, \phi_1, \ldots, \phi_n \vdash \psi$. Llamamos *secuente*[7] a esta expresión y *cálculo de secuentes* a la representación de todo el aparato lógico.

[7] En algunos textos se distingue entre *secuente sintáctico*, éste, y *secuente semántico*, la implicación lógica, $\phi_0, \phi_1, \ldots, \phi_n \vDash \psi$.

§ 2.2.1 Reglas deductivas derivadas (RD)

Aunque con las ocho reglas deductivas básicas es posible resolver cualquier problema de deducción formal, el proceso, a veces, sería bastante arduo. Puede facilitarse esta labor aumentando el número de reglas que puedan utilizarse, las denominadas *reglas derivadas*, de las anteriores.

Conceptos que ayudan a la generación de estas reglas derivadas son:

- derivación formal[8] y regla de sustitución[9], en el campo sintáctico, y
- teorema de sustitución[10], formas normales[11] y dualidad[12], en el campo semántico.

Pues bien, debido a que la lógica de juntores es correcta y completa[13]:

0.º, todas las implicaciones lógicas $\phi \vDash \psi$ —campo semántico— (y hemos estudiado bastantes hasta este momento), son reglas deductivas $\phi \vdash \psi$ —campo sintáctico—, y de manera similar,

1.º, todas las equivalencias lógicas $\phi \equiv \psi$ —campo semántico— son reglas deductivas dobles $\phi \dashv\vdash \psi$ —campo sintáctico—, esto es, reglas deductivas en la forma $\phi \vdash \psi$ y sus recíprocas en la forma $\phi \dashv \psi$ —que también son, en dicho caso, reglas deductivas—; en particular, todas las correspondientes a interdefinición de juntores estudiadas en anteriores ejemplos[14] y teoremas[15].

Estas reglas deductivas dobles las notaremos:

$$\phi \dashv\vdash \psi \qquad \text{o} \qquad \frac{\phi}{\psi}$$

Por ejemplo, las *leyes de* De Morgan:

$$p \wedge q \dashv\vdash \neg(\neg p \vee \neg q) \qquad \text{o} \qquad \frac{p \wedge q}{\neg(\neg p \vee \neg q)}$$

$$\begin{aligned}
p \wedge q &\dashv\vdash \neg(\neg p \vee \neg q)\\
p \vee q &\dashv\vdash \neg(\neg p \wedge \neg q)\\
\neg(p \wedge q) &\dashv\vdash \neg p \vee \neg q\\
\neg(p \vee q) &\dashv\vdash \neg p \wedge \neg q\\
\neg(p_0 \wedge p_1 \wedge \cdots \wedge p_n) &\dashv\vdash \neg p_0 \vee \neg p_1 \vee \cdots \vee \neg p_n\\
\neg(p_0 \vee p_1 \vee \cdots \vee p_n) &\dashv\vdash \neg p_0 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n
\end{aligned}$$

[8] *Vid. supra* § 2.0 (pág. 177 de esta edición).
[9] *Vid. infra* observación 2.2.34 (pág. 213 de esta edición).
[10] *Vid. supra* § 1.19 (pág. 160 de esta edición).
[11] *Vid. infra* § 3.1 (pág. 257 de esta edición).
[12] *Vid. infra* § 3.2 (pág. 272 de esta edición).
[13] *Vid. infra* teorema 6.9 (pág. 446 de esta edición).
[14] *Vid. supra* ejemplos 101, 105, 106 y 107 (págs. 157, 161, 162 y 163, respectivamente, de esta edición).
[15] *Vid. supra* teoremas 1.25 y 1.27 (págs. 165 y 166, respectivamente, de esta edición).

el *principio de* FILÓN:

$$p \to q \dashv\vdash \neg p \vee q\,,$$

y el *principio de* CRISIPO:

$$p \to q \dashv\vdash \neg(p \wedge \neg q)\,.$$

Como en el caso de las reglas básicas, proporcionamos su nombre y figura, con la abreviatura correspondiente si es el caso. Por otro lado, algunas actividades consistirán en hallar la fundamentación de algunas de estas reglas.

Reglas derivadas iniciales

De negación

Teorema 2.5 (RD de negación)

Introducción de doble negación (IDN):

$$\frac{\phi}{\neg\neg\phi}$$

Doble negación (DN):

$$\frac{\neg\neg\phi}{\phi} \quad \text{(doble línea)}$$

De negación y disyunción

Teorema 2.6 (RD de negación y disyunción)

Principio del tercio excluso
(*Tertium non datur*) (*Principium tertii exclusi*) (PTE):

$$\frac{\top}{\phi \vee \neg\phi} \quad \text{(doble línea)}$$

Regla de resolución (RES)

$$\frac{\begin{array}{l}\phi \vee \chi \\ \psi \vee \neg\chi\end{array}}{\phi \vee \psi}$$

Observación 2.2.4.— Sobre PTE:

0. El principio del tercio excluso suele enunciarse también como la regla sin premisa

$$\phi \vee \neg\phi.$$

1. El principio del tercio excluso pudiese interpretarse, en un sentido, como una *regla de introducción de* $\top$ (I$\top$),

$$\frac{\phi \vee \neg\phi}{\top}$$

y, en el otro sentido, como una *regla de eliminación de* $\top$ (E$\top$),

$$\frac{\top}{\phi \vee \neg\phi}$$

lo que permitiría considerar la constante enunciativa $\top$ como un operador lógico —un juntor medádico—, en consonancia con la composición medádica tautología[16].

Observación 2.2.5.— Sobre RES:

0. En la regla de resolución, la conclusión, la cláusula $\phi \vee \psi$ se conoce como la *resolvente* de las cláusulas $\phi \vee \chi$ y $\psi \vee \neg\chi$.

1. *Modus ponens* es un caso particular de RES[17].

2. A modo de ejemplo, algunos otros casos particulares de RES son:

$$\begin{array}{ccccc} \text{RES}_0 & \text{RES}_1 & \text{RES}_2 & \text{RES}_3 & \text{RES}_4 \\ \phi \vee \chi & \chi & \chi & \phi \vee \chi & \neg\phi \vee \chi \\ \underline{\phi \vee \neg\chi} & \underline{\psi \vee \neg\chi} & \underline{\neg\chi} & \underline{\neg\phi \vee \neg\chi} & \underline{\psi \vee \neg\chi} \\ \phi & \psi & \bot & \top & \neg\phi \vee \psi \end{array}$$

(observemos que este último, en otras palabras (formalmente, por la regla de sustitución[18]), es $\phi \to \chi, \chi \to \psi$, con resolvente $\phi \to \psi$).

3. La regla de resolución es ampliamente utilizada en *demostración automática de teoremas*.

Ejemplo 124

Demostremos por reducción al absurdo (RAA) que se satisface

$$\{(\neg\phi \vee \psi), (\neg\psi \vee \chi), \neg\chi\} \vdash \neg\phi;$$

hagámoslo por derivación formal utilizando profusamente la regla de resolución.

Resolución.— En efecto:

16 *Cfr. supra* § 1.3.0 (pág. 78 de esta edición).
17 *Vid. infra* § 125 (pág. 213 de esta edición).
18 *Cfr. infra* teorema 2.33 (pág. 213 de esta edición).

0.	$\neg\phi \vee \psi$	[DF0] Premisa
1.	$\neg\psi \vee \chi$	[DF0] Premisa
2.	$\neg\chi$	[DF0] Premisa
3.	ϕ	Supuesto
4.	$\neg\psi$	[DF2] RES_1 2, 1
5.	$\neg\phi$	[DF2] RES_1 4, 0
6.	$\bot$	[DF2] RES_0 3, 5
7.	$\neg\phi$	[DF2] RAA 3–6

■

De negación y conjunción

Teorema 2.7 (RD de negación y conjunción)

Principio de la no contradicción (PNC) (*Principium contradictionis*):

$$\frac{\bot}{\phi \wedge \neg\phi}$$

Eliminación débil de la negación (*Ex contradictione quodlibet* (ECQ)):

$$\frac{\phi \wedge \neg\phi}{\psi}$$

Observación 2.2.6.— 0. El principio de la no contradicción suele enunciarse también como la regla sin premisa

$$\neg(\phi \wedge \neg\phi).$$

1. El principio de la no contradicción pudiese interpretarse como una *regla de introducción de* $\bot$ (I$\bot$),

$$\frac{\phi \quad \neg\phi}{\bot}$$

a la vez que del principio de la (no) contradicción y de la eliminación débil de la negación, aplicando la regla de sustitución, pudiese derivarse una *regla de eliminación de* $\bot$ (E$\bot$),

$$\frac{\bot}{\phi}$$

lo cual permitiría considerar la constante enunciativa $\bot$ como un operador lógico —un juntor medádico—, en consonancia con la composición medádica contradicción[19].

Observación 2.2.7.— Además de *Ex contradictione quodlibet* (de la contradicción, cualquier cosa), la ley de eliminación débil de la negación también es conocida como *Ex falso quodlibet* (de la falsedad, cualquier cosa) y como el *principio de explosión*.

[19] *Cfr. supra* § 1.3.0 (pág. 78 de esta edición).

De implicación

Teorema 2.8 (RD de implicación)

Silogismo Barbara, 1.ª forma:

$$\frac{\phi \to \psi}{(\psi \to \chi) \to (\phi \to \chi)}$$

Silogismo Barbara, 2.ª forma
(Ley del silogismo hipotético (Sil))
(Transitividad de → como operación):

$$\frac{\phi \to \psi \qquad \psi \to \chi}{\phi \to \chi}$$

Mutación de premisas (MPr):

$$\frac{\phi \to (\psi \to \chi)}{\psi \to (\phi \to \chi)} \quad (\text{doble línea})$$

Identidad (Id)
(Ley de repetición):

$$\frac{\phi}{\phi} \quad (\text{doble línea})$$

Carga de premisa (CPr)
(Ley de introducción del antecedente):

$$\frac{\phi}{\psi \to \phi}$$

Observación 2.2.8.— Mediando la regla de sustitución[20], la ley de identidad (Id) pudiese interpretarse, en un sentido, como una *regla de introducción de* id (Iid),

$$\frac{\phi}{\mathrm{id}\phi}$$

y, en el otro sentido, como una *regla de eliminación de* id (Eid),

$$\frac{\mathrm{id}\phi}{\phi}$$

en consonancia con la funcionalidad de id como operador lógico, el juntor monádico afirmador[21].

De negación e implicación

Teorema 2.9 (RD de negación e implicación, I)

Modus tollendo tollens (MTT):

$$\frac{\phi \to \psi \qquad \neg\psi}{\neg\phi}$$

[20] *Vid. infra* observación 2.2.34 (pág. 213 de esta edición).
[21] *Cfr. supra* § 1.3.1 (pág. 80 de esta edición).

Observación 2.2.9.— La regla *modus tollendo tollens* —modo que negando, niega— también se conoce como *modus tollens* —modo que niega— y se abrevia MT. Como dijimos[22], tradicionalmente es una figura del llamado *silogismo hipotético* (SH_1). Su esquema argumental es

$$\begin{array}{rl} & \text{Se tiene que } \phi \to \psi. \\ & \text{Se tiene } \neg\psi. \\ \hline \therefore & \text{Se sigue } \neg\phi. \end{array}$$

Teorema 2.10 (RD de negación e implicación, II)

Ley de los contrapuestos (Cp_0): $$\frac{\phi \to \psi}{\neg\psi \to \neg\phi}$$

Contraposición constructiva (Cp_1): $$\frac{\phi \to \neg\psi}{\psi \to \neg\phi}$$

Contraposición clásica (Cp_2): $$\frac{\neg\phi \to \psi}{\neg\psi \to \phi}$$

Recíproca de la ley de los contrapuestos (Cp_3): $$\frac{\neg\phi \to \neg\psi}{\psi \to \phi}$$

Observación 2.2.10.— Fusionamos las reglas Cp_0 y Cp_3 en

Ley de contraposición (Cp): $$\begin{array}{c} \phi \to \psi \\ \hline\hline \neg\psi \to \neg\phi \end{array}$$

Observación 2.2.11.— Notemos que en cualquier momento, pudiésemos incrementar el grado de abstracción de las reglas; por ejemplo, también pudiésemos llamar ley de contraposición (Cp) a

$$\begin{array}{c} \phi \vdash \psi \\ \hline\hline \neg\psi \vdash \neg\phi \end{array}$$

Observación 2.2.12.— Con respecto a la eliminación débil de la negación (ECQ)[23], también aparece en algunos textos la siguiente figura alternativa, basada en el negador y el implicador,

$$\frac{\neg\phi}{\phi \to \psi}$$

y las siguientes dos variantes, también basadas en el negador y el implicador,

[22] *Cfr. supra* ejemplo 115 (pág. 181 de esta edición).
[23] *Cfr. supra* teorema 2.7 (pág. 197 de esta edición).

Ex contradictione irrestricta:

$$\frac{\phi \to \psi \qquad \phi \to \neg\psi}{\phi \to \chi}$$

Ex contradictione negativa:

$$\frac{\phi \to \psi \qquad \phi \to \neg\psi}{\phi \to \neg\chi}$$

Reglas derivadas adicionales

De negación y disyunción

Teorema 2.11 (RD de negación y disyunción)

Silogismo disyuntivo (SD_0)
Modus tollendo ponens (MTP_0):

$$\frac{\phi \vee \psi \qquad \neg\psi}{\phi}$$

Silogismo disyuntivo (SD_1)
Modus tollendo ponens (MTP_1):

$$\frac{\phi \vee \psi \qquad \neg\phi}{\psi}$$

Observación 2.2.13.— SD_0 y SD_1 corresponden justamente a las dos modalidades de *Modus tollendo ponens* (MTP) —«modo que negando, afirma»—, según el consecuente sea ϕ o ψ. Por ello también MTP_0 y MTP_1 las designan. Los esquemas argumentales respectivos de dichas modalidades son:

	Se tiene $\phi \vee \psi$.		Se tiene $\phi \vee \psi$.
	Se tiene $\neg\psi$.		Se tiene $\neg\phi$.
$\therefore$	Se sigue ϕ.	$\therefore$	Se sigue ψ.

De contravalencia

Eliminación

Teorema 2.12 (RD de contravalencia, I)

Eliminación de la contravalencia (ECV_0)
Silogismo contravalente (SC_{00})
Modus ponendo tollens (MPT_0):

$$\frac{\phi \veebar \psi \qquad \phi}{\neg\psi}$$

Eliminación de la contravalencia (ECV_1)
Silogismo contravalente (SC_{01})
Modus ponendo tollens (MPT_1):

$$\frac{\phi \veebar \psi \qquad \psi}{\neg\phi}$$

Observación 2.2.14.— Las reglas ECV_0 y ECV_1 corresponden justamente a las dos modalidades de *Modus ponendo tollens* (MPT) —«modo que afirmando, niega»—, según el consecuente sea $\neg\psi$ o $\neg\phi$. Por ello también MPT_0 y MPT_1 las designan. Como ya hemos comentado[24], tradicionalmente son las dos modalidades de la primera figura del *silogismo contravalente*, SC_{00} y SC_{01}, respectivamente. Los esquemas argumentales respectivos de dichas modalidades son:

	Se tiene $\phi \veebar \psi$.		Se tiene $\phi \veebar \psi$.
	Se tiene ϕ.		Se tiene ψ.
$\therefore$	Se sigue $\neg\psi$.	$\therefore$	Se sigue $\neg\phi$.

en oposición al *silogismo disyuntivo*, de única figura, cuyos esquemas argumentales respectivos de sus dos modalidades, SD_0 y SD_1, hemos estudiado en la observación inmediatamente anterior.

Introducción y eliminación

Hemos eliminado el contravaledor, mas no lo hemos introducido. Hagámoslo ahora y, de paso, veamos nuevas reglas de eliminación.

[24] *Cfr. supra* ejemplo 116 (pág. 182 de esta edición).

Teorema 2.13 (RD de contravalencia, II)

Introducción del contravaledor (ICV_0):
$$\frac{\phi \vee \psi \qquad \neg\phi \vee \neg\psi}{\phi \veebar \psi}$$

Eliminación del contravaledor (ECV_2):
$$\frac{\phi \veebar \psi}{\phi \vee \psi}$$

Eliminación del contravaledor (ECV_3):
$$\frac{\phi \veebar \psi}{\neg\phi \vee \neg\psi}$$

Observación 2.2.15.— Las reglas ICV_0, ECV_2 y ECV_3 se fusionan en

Ley de contravalencia (CV):
$$\frac{\phi \vee \psi \qquad \neg\phi \vee \neg\psi}{\phi \veebar \psi} \text{ (doble)}$$

La regla deductiva doble *ley de contravalencia* (CV) se corresponde con la *forma normal conjuntiva* (FNC)[25] de $\phi \veebar \psi$.

Introducción

Finalmente, veamos dos reglas más de introducción, ahora, con las bases $\{\neg, \vee\}$ y $\{\neg, \vee, \wedge\}$.

Teorema 2.14 (RD de contravalencia, III)

Introducción de $\veebar$ a partir de $\neg$ y $\vee$ (ICV_1):
$$\frac{\neg(\neg\phi \vee \psi) \vee \neg(\phi \vee \neg\psi)}{\phi \veebar \psi} \text{ (doble)}$$

Teorema 2.15 (RD de contravalencia, IV)

Introducción de $\veebar$ a partir de $\neg$, $\vee$ y $\wedge$ (ICV_2):
$$\frac{(\phi \wedge \neg\psi) \vee (\neg\phi \wedge \psi)}{\phi \veebar \psi} \text{ (doble)}$$

Observación 2.2.16.— Esta regla deductiva doble ICV_2 se corresponde:

- con la *forma normal disyuntiva* (FND)[26] de $\phi \veebar \psi$, y

[25] *Vid. infra* § 3.1.0 (págs. 258ss. de esta edición).
[26] *Vid. infra* § 3.1.0 (págs. 258ss. de esta edición).

- con la regla semántica *falsedad de la equivalencia* (FE)[27].

De conjunción e implicación

Teorema 2.16 (RD de conjunción e implicación)

Ley de importación (Imp):
$$\frac{\phi \to (\psi \to \chi)}{\phi \land \psi \to \chi}$$

Ley de exportación (Exp):
$$\frac{\phi \land \psi \to \chi}{\phi \to (\psi \to \chi)}$$

Observación 2.2.17.— En la literatura aparece, a veces, como ley de importación la fusión de las dos anteriores:

Ley de importación (LI):
$$\frac{\phi \land \psi \to \chi}{\phi \to (\psi \to \chi)}$$

Sobre la ley de importación

La mente matemática, por naturaleza o educada, peca de ambición generalizadora. Pudiésemos ver la ley de importación como un caso particular de la acción de una relación diádica R no necesariamente simétrica (ley de importación/exportación) entre dos términos funcionales:

$$f(g(x,y),z)\ R\ f(x,f(y,z)), \tag{2.2}$$

donde R, por ejemplo, bien pudiese ser de equivalencia lógica y expresarse

$$f(g(x,y),z) \text{ si, y sólo si, } f(x,f(y,z))$$

o de igualdad numérica y expresarse

$$f(g(x,y),z) = f(x,f(y,z)).$$

[27] *Vid. infra* § 3.3.0 (págs. 275ss. de esta edición) y § 366 (págs. 381ss. de esta edición).

De disyunción e implicación

Teorema 2.17 (RD de disyunción e implicación)

Dilema constructivo simple (DCS):

$$\frac{\phi \lor \psi \quad \phi \to \chi \quad \psi \to \chi}{\chi}$$

Dilema constructivo complejo (DCC):

$$\frac{\phi \lor \psi \quad \phi \to \chi \quad \psi \to \theta}{\chi \lor \theta}$$

De negación, disyunción e implicación

Teorema 2.18 (RD de negación, disyunción e implicación)

Dilema destructivo simple (DDS):

$$\frac{\neg\phi \lor \neg\psi \quad \chi \to \phi \quad \chi \to \psi}{\neg\chi}$$

Dilema destructivo complejo (DDC):

$$\frac{\neg\phi \lor \neg\psi \quad \chi \to \phi \quad \theta \to \psi}{\neg\chi \lor \neg\theta}$$

De la coimplicación

Introducción y eliminación del coimplicador, I

A continuación las tradicionales reglas de introducción y eliminación del coimplicador, en relación con el implicador.

Teorema 2.19 (RD de coimplicación, I)

Introducción del coimplicador (ICO_0):

$$\frac{\begin{array}{c}\phi \rightarrow \psi \\ \psi \rightarrow \phi\end{array}}{\phi \leftrightarrow \psi}$$

Eliminación del coimplicador
(Debilitación implicativa) (ECO_0):

$$\frac{\phi \leftrightarrow \psi}{\phi \rightarrow \psi}$$

Eliminación del coimplicador
(Debilitación replicativa) (ECO_1):

$$\frac{\phi \leftrightarrow \psi}{\psi \rightarrow \phi}$$

Observación 2.2.18.— Las reglas ICO, ECO_0 y ECO_1 se fusionan en

Ley de coimplicación (CO):

$$\frac{\begin{array}{c}\phi \rightarrow \psi \\ \psi \rightarrow \phi\end{array}}{\phi \leftrightarrow \psi}$$

Si el SDN se definiese a partir de la base de juntores $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$, entonces, el conjunto de reglas básicas constaría, en vez de ocho reglas, de diez, al incorporar las reglas de introducción del coimplicador (ICO) y de eliminación del coimplicador —en sus dos modalidades ECO_0 y ECO_1— o de nueve reglas, al incorporar su fusión, la regla de coimplicación (CO).

Introducción y eliminación del coimplicador, II

Alternativamente, son posibles otras reglas de introducción y eliminación del coimplicador para tener una definición alternativa del SDN similar a la comentada en la observación anterior. Destacamos tres, las vistas anteriormente, en relación con el implicador, las que presentamos a continuación en, relación con el conjuntor, y las que mostraremos en el apartado siguiente, en relación con el disyuntor.

Teorema 2.20 (RD de coimplicación, II)

Introducción del coimplicador (ICO_1)::

$$\frac{\neg(\phi \land \neg\psi) \quad \neg(\neg\phi \land \psi)}{\phi \leftrightarrow \psi}$$

Eliminación del coimplicador ($ECCO_2$):

$$\frac{\phi \leftrightarrow \psi}{\neg(\phi \land \neg\psi)}$$

Eliminación del coimplicador ($ECCO_3$):

$$\frac{\phi \leftrightarrow \psi}{\neg(\neg\phi \land \psi)}$$

Observación 2.2.19.— Las reglas ICO_1, ECO_2 y ECO_3 se fusionan en

Ley de coimplicación (RCO_1):

$$\frac{\neg(\phi \land \neg\psi) \quad \neg(\neg\phi \land \psi)}{\phi \leftrightarrow \psi}$$

Introducción y eliminación del coimplicador, III

Presentamos otras reglas alternativas de introducción y eliminación del coimplicador, esta vez en relación con el disyuntor.

Teorema 2.21 (RD de coimplicación, III)

Introducción del coimplicador (ICO_2):

$$\frac{\neg\phi \lor \psi \quad \phi \lor \neg\psi}{\phi \leftrightarrow \psi}$$

Teorema 2.22 (RD de coimplicación, IV)

Eliminación del coimplicador (ECO_4):

$$\frac{\phi \leftrightarrow \psi}{\neg\phi \lor \psi}$$

Eliminación del coimplicador (ECO_5):

$$\frac{\phi \leftrightarrow \psi}{\phi \lor \neg\psi}$$

Observación 2.2.20.— Las reglas ICO_2, ECO_4 y ECO_5 se fusionan en

Ley de coimplicación (RCO_2):

$$\frac{\neg\phi \lor \psi \quad \phi \lor \neg\psi}{\phi \leftrightarrow \psi}$$

Introducción del coimplicador

Ahora, con las bases $\{\neg, \vee\}$ y $\{\neg, \vee, \wedge\}$.

Teorema 2.23 (RD de coimplicación, V)

Introducción de $\leftrightarrow$ a partir de $\neg$ y $\vee$ (ICO_3):

$$\frac{\neg(\neg\phi \vee \neg\psi) \vee \neg(\phi \vee \psi)}{\phi \leftrightarrow \psi}$$

Introducción de $\leftrightarrow$ a partir de $\neg$, $\vee$ y $\wedge$ (ICO_4):

$$\frac{(\phi \wedge \psi) \vee (\neg\phi \wedge \neg\psi)}{\phi \leftrightarrow \psi}$$

Observación 2.2.21.— La regla deductiva doble ICO_4 se corresponde con la regla semántica *verdad de la equivalencia* (VE)[28].

Regla de separación del coimplicador

En sus dos modalidades.

Teorema 2.24 (RD de coimplicación, VI)

Regla de separación ($RSCO_0$):

$$\frac{\phi \leftrightarrow \psi \quad \phi}{\psi}$$

Regla de separación ($RSCO_1$):

$$\frac{\phi \leftrightarrow \psi \quad \psi}{\phi}$$

Más reglas derivadas: algunas propiedades de los juntores como relaciones

La relación de implicación

Teorema 2.25 (Propiedades de la implicación como relación)

Reflexiva: $\phi \to \phi$

Transitiva (Sil):

$$\frac{(\phi \to \psi) \wedge (\psi \to \chi)}{\phi \to \chi}$$

Observación 2.2.22.— La relación $\to$ de implicación es una relación de preorden parcial[29] en la colección $\mathcal{F}_0$ de todas las fórmulas de la lógica de juntores.

[28] *Vid. infra* § 3.3.0 (págs. 275ss. de esta edición) y § 366 (págs. 381ss. de esta edición).
[29] *Cfr. infra* definición 11.50 (pág. 645 de esta edición).

La relación de coimplicación

Teorema 2.26 (Propiedades de $\leftrightarrow$ como relación)

Reflexividad de la coimplicación (RCO): $\phi \leftrightarrow \phi$

Simetría de la coimplicación (SCO)
(Regla de inversión):

$$\frac{\phi \leftrightarrow \psi}{\psi \leftrightarrow \phi}$$

Transitividad de la coimplicación (TCO):

$$\frac{\begin{array}{c}\phi \leftrightarrow \psi \\ \psi \leftrightarrow \chi\end{array}}{\phi \leftrightarrow \chi}$$

Observación 2.2.23.— La relación $\leftrightarrow$ de coimplicación es una relación de equivalencia[30] en la colección $\mathcal{F}_0$ de todas las fórmulas de la lógica de juntores.

Más reglas derivadas: algunas propiedades de los juntores como operaciones

La operación disyunción

Teorema 2.27 (Propiedades de la disyunción como operación)

Conmutativa de la disyunción (CoD):

$$\frac{\phi \lor \psi}{\overline{\psi \lor \phi}}$$

Asociativa de la disyunción (AD):

$$\frac{(\phi \lor \psi) \lor \chi}{\overline{\phi \lor (\psi \lor \chi)}}$$

Elemento neutro de la disyunción (eNtrD):

$$\frac{\phi \lor \bot}{\overline{\phi}}$$

Elemento absorbente de la disyunción (eAbsD):

$$\frac{\phi \lor \top}{\overline{\top}}$$

Idempotencia de la disyunción (IdD):

$$\frac{\phi \lor \phi}{\overline{\phi}}$$

Demostración.— (Por ahora, sólo AD, la asociativa de la disyunción).

[30] *Cfr. infra* definición 11.39 (pág. 628 de esta edición).

0.	$(p \vee q) \vee r$	Premisa
1.	$(p \vee q)$	Supuesto
2.	p	Supuesto
3.	$p \vee (q \vee r)$	ID_0 2
4.	q	Supuesto
5.	$q \vee r$	ID_0 4
6.	$p \vee (q \vee r)$	ID_1 5
7.	$p \vee (q \vee r)$	Cas 1, 2–3, 4–6
8.	r	Supuesto
9.	$q \vee r$	ID_1 8
10.	$p \vee (q \vee r)$	ID_1 9
11.	$p \vee (q \vee r)$	Cas 0, 1–7, 8–10

■

Observación 2.2.24.— $(\mathcal{F}_0; \vee)$ tiene estructura de monoide abeliano idempotente[31].

La operación conjunción

Teorema 2.28 (Propiedades de la conjunción como operación)

Conmutativa de la conjunción (CoC): $$\frac{\phi \wedge \psi}{\psi \wedge \phi}$$

Asociativa de la conjunción (AC): $$\frac{(\phi \wedge \psi) \wedge \chi}{\phi \wedge (\psi \wedge \chi)}$$

Elemento neutro de la conjunción (eNtrC): $$\frac{\phi \wedge \top}{\phi}$$

Elemento absorbente de la conjunción (eAbsC): $$\frac{\phi \wedge \bot}{\bot}$$

Idempotencia de la conjunción (IdC): $$\frac{\phi \wedge \phi}{\phi}$$

Observación 2.2.25.— $(\mathcal{F}_0; \wedge)$ tiene estructura de monoide abeliano idempotente[32].

[31] *Cfr. infra* § 17.4 (pág. 842 de esta edición).
[32] *Cfr. infra* § 17.4 (pág. 842 de esta edición).

Observación 2.2.26.— Notemos que debido a la propiedad asociativa de un juntor, es posible suprimir paréntesis en ciertas ocasiones; por ejemplo, en el caso de la disyunción y de la conjunción, las deducciones directas y recíproca, esto es, las propias reglas AD y AC, nos permiten expresar la equivalencia de las expresiones

$$(\phi \vee \psi) \vee \chi \dashv\vdash \phi \vee (\psi \vee \chi) \dashv\vdash \phi \vee \psi \vee \chi$$
$$(\phi \wedge \psi) \wedge \chi \dashv\vdash \phi \wedge (\psi \wedge \chi) \dashv\vdash \phi \wedge \psi \wedge \chi$$

y trabajar habitualmente con estas últimas, al darse la equivalencia en todas las posibles situaciones correctas de paréntesis.

Observación 2.2.27.— La asociatividad de la disyunción y de la conjunción permite expresar versiones para más de dos fórmulas de reglas vistas, por ejemplo, las leyes de De Morgan y la Ley de Resolución,

Distribución de ¬ en ∨ (DM_0):
$$\frac{\neg(\phi_0 \vee \phi_1 \vee \cdots \vee \phi_k)}{\neg\phi_0 \wedge \neg\phi_1 \wedge \cdots \wedge \neg\phi_k}$$

Distribución de ¬ en ∧ (DM_1)
(Dual de DM_0, esto es, DM_0'):
$$\frac{\neg(\phi_0 \wedge \phi_1 \wedge \cdots \wedge \phi_k)}{\neg\phi_0 \vee \neg\phi_1 \vee \cdots \vee \neg\phi_k}$$

Regla de resolución (Res)
$$\frac{\begin{array}{l}\phi_0 \vee \phi_1 \vee \cdots \vee \phi_k \vee \chi \\ \psi_0 \vee \psi_1 \vee \cdots \vee \psi_k \vee \neg\chi\end{array}}{\phi_0 \vee \phi_1 \vee \cdots \vee \phi_k \vee \psi_0 \vee \psi_1 \vee \cdots \vee \psi_k}$$

La disyunción y la conjunción como operaciones, conjuntamente

Teorema 2.29 (Propiedades conjuntas de ∨ y ∧ como operaciones)

Absorción de ∨ por ∧ (AbsC):
$$\frac{\phi \wedge (\phi \vee \psi)}{\phi}$$

Absorción de ∧ por ∨ (AbsD)
(Dual de AbsC, que pudiese designarse por AbsC′):
$$\frac{\phi \vee (\phi \wedge \psi)}{\phi}$$

Distributiva de ∧ en ∨ (DisC):
$$\frac{\phi \wedge (\psi \vee \chi)}{(\phi \wedge \psi) \vee (\phi \wedge \chi)}$$

Distributiva de ∨ en ∧ (DisD)
(Dual de DisC, que pudiese designarse por DisC′):
$$\frac{\phi \vee (\psi \wedge \chi)}{(\phi \vee \psi) \wedge (\phi \vee \chi)}$$

Observación 2.2.28.— A modo de ilustración de las propiedades asociativa y distributiva en acción.

$$
\begin{aligned}
& s \vee \big((p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q)\big) \\
\dashv\vdash\ & (s \vee (p \vee q)) \wedge (s \vee (\neg p \vee q)) \wedge (s \vee (p \vee \neg q)) \wedge (s \vee (\neg p \vee \neg q)) && \text{(por RD distributiva)} \\
\dashv\vdash\ & (s \vee p \vee q) \wedge (s \vee \neg p \vee q) \wedge (s \vee p \vee \neg q) \wedge (s \vee \neg p \vee \neg q) && \text{(por RD asociativa)}
\end{aligned}
$$

Observación 2.2.29.— Veamos una nueva combinación de la acción de las propiedades asociativa y distributiva (sólo se muestra el resultado final; sin duda es interesante pensar y documentar los pasos intermedios) (*cfr.* actividad 2.2 [pág. 211 de esta edición]).

$$(p \vee q) \wedge (r \vee s) = \ldots = (p \overset{①}{\wedge} r) \vee (p \overset{②}{\wedge} s) \vee (q \overset{③}{\wedge} r) \vee (q \overset{④}{\wedge} s)$$

Observación 2.2.30.— $(\mathcal{F}_0; \wedge, \vee, \neg)$ tiene estructura de álgebra de Boole[33].

Actividad 2.2

Documentemos los pasos intermedios de $(p \vee q) \wedge (r \vee s) = \ldots = (p \wedge r) \vee (p \wedge s) \vee (q \wedge r) \vee (q \wedge s)$.

La operación implicación

Teorema 2.30 (Propiedades de la implicación como operación)

Recíproca de la idempotencia:
$$\frac{\phi}{\phi \to \phi}$$

Distributiva (de la implicación en sí misma):
$$\frac{\phi \to (\psi \to \chi)}{(\phi \to \psi) \to (\phi \to \chi)} \quad \text{(doble línea)}$$

Observación 2.2.31.— Se satisface

$$(\phi \to \psi) \to \chi \vdash \phi \to (\psi \to \chi).$$

[33] *Cfr. infra* § 3.7 (pág. 353 de esta edición).

Hay quienes se refieren a este hecho como asociatividad de izquierda a derecha (observemos la posición de los paréntesis) y quienes la llaman simplemente asociatividad izquierda. Por otro lado,

$$\phi \to (\psi \to \chi) \nvdash (\phi \to \psi) \to \chi.$$

En otras palabras, la operación implicación como operación no es asociativa. Considerando ambos resultados, hay quienes dicen que es asociativa de derecha a izquierda, pero no de izquierda a derecha, y quienes dicen que es asociativa izquierda, pero no asociativa derecha.

La operación coimplicación

Teorema 2.31 (Propiedades de $\leftrightarrow$ como operación, I)

Conmutatividad de la coimplicación (CoCO): $$\frac{\phi \leftrightarrow \psi}{\psi \leftrightarrow \phi}$$ (doble línea)

Asociatividad de la coimplicación (ACO): $$\frac{(\phi \leftrightarrow \psi) \leftrightarrow \chi}{\phi \leftrightarrow (\psi \leftrightarrow \chi)}$$ (doble línea)

Elemento neutro de la coimplicación (eNtrCO): $$\frac{\phi \leftrightarrow \top}{\phi}$$ (doble línea)

Elemento simétrico para la coimplicación (eSimCO): $$\frac{\top}{\phi \leftrightarrow \phi}$$ (doble línea)

Observación 2.2.32.— $(\mathcal{F}_0; \leftrightarrow)$ tiene estructura de grupo abeliano[34].

Teorema 2.32 (Propiedades de $\leftrightarrow$ como operación, II)

Recíproca de la idempotencia de la coimplicación (ReIdCO): $$\frac{\phi}{\phi \leftrightarrow \phi}$$

Absorción de $\leftrightarrow$ (AbsCO): $$\frac{\phi \leftrightarrow (\phi \to \psi)}{\phi}$$

Distributiva de $\to$ en $\leftrightarrow$: $$\frac{\phi \to (\psi \leftrightarrow \chi)}{(\phi \to \psi) \leftrightarrow (\phi \to \chi)}$$ (doble línea)

[34] *Cfr. infra* § 17.5 (pág. 849 de esta edición).

Reglas (derivadas) de intercambio y sustitución

Teorema 2.33 (Intercambio y sustitución)

Regla de intercambio (I):

$$\frac{\begin{array}{l}\chi \leftrightarrow \tau\\ \phi_\chi\end{array}}{\phi_\tau}$$

Regla de sustitución (S):

$$\frac{\phi_s \leftrightarrow \top}{\phi_\tau \leftrightarrow \top}$$

Observación 2.2.33.— La regla de intercambio se corresponde con la operación de intercambio y refleja lo establecido por el *teorema de intercambio*[35]. La *regla de intercambio* afirma que dadas dos fórmulas equivalentes χ y τ, si una fórmula ϕ contiene como subfórmula a χ (hecho que notamos ϕ_χ) y se reemplaza una ocurrencia determinada, digamos la primera, de χ en ϕ por τ, entonces el resultado es una fórmula ϕ_τ, lógicamente equivalente a ϕ_χ. Por ejemplo, si ϕ_χ es $\neg(\neg p \vee \neg q) \rightarrow (\neg p \wedge q)$, y χ es $\neg(\neg p \vee \neg q)$, y τ es $p \wedge q$, y reemplazamos χ por τ, se obtiene como ϕ_τ, $(p \wedge q) \rightarrow (\neg p \wedge q)$, que es lógicamente equivalente a ϕ_χ. Es decir,

$$\frac{\begin{array}{l}\chi \leftrightarrow \tau\\ \phi_\chi\end{array}}{\phi_\tau \wedge (\phi_\chi \leftrightarrow \phi_\tau)}$$

de donde se extrae, en particular, la regla de intercambio.

Observación 2.2.34.— La regla de sustitución (campo sintáctico) se corresponde con el *teorema de sustitución*[36] (campo semántico). La *regla de sustitución* afirma que si una proposición compuesta ϕ_s es una fórmula válida y si cada vez que aparece una variable de ϕ_s, digamos s, se sustituye por una proposición τ, siempre la misma, entonces el resultado es una proposición compuesta ϕ_τ que también es una fórmula válida. Por ejemplo, si ϕ_s es $(p \wedge (p \rightarrow q)) \rightarrow q$, que es una fórmula válida, y τ es $q \rightarrow r$, y reemplazamos p —la «s» en este ejemplo— por τ, se obtiene como ϕ_τ, $((q \rightarrow r) \wedge ((q \rightarrow r) \rightarrow q)) \rightarrow q$, que también es una fórmula válida.

Ejemplo 125

Demostremos que *modus ponens* es un caso particular de la regla de resolución (RES) (*cfr. supra* teorema 2.6 [pág. 195 de esta edición]).

[35] *Vid. supra* teorema 1.17 (pág. 158 de esta edición).
[36] *Vid. supra* teorema 1.19 (pág. 160 de esta edición).

Resolución.— En efecto, *modus ponens*,

$$\begin{array}{l} \phi \to \psi \\ \phi \\ \hline \psi \end{array}$$

es un caso particular de RES, ya que $\phi \to \psi$ es equivalente a $\neg\phi \vee \psi$ y aplicando la regla de sustitución en la primera premisa, la regla de resolución queda justamente *modus ponens*:

$$\begin{array}{l} \neg\phi \vee \psi \\ \phi \\ \hline \psi \end{array}$$

■

Absurdos: reglas (derivadas) *Consequentia mirabilis* y *Reductio ad absurdum*

Teorema 2.34

Ley de Clavio (*Consequentia mirabilis*):

$$\begin{array}{l} \neg\phi \to \phi \\ \hline \phi \end{array}$$

Observación 2.2.35.— La ley de Clavio establece la verdad de una proposición a partir de la inconsistencia de su negación.

Teorema 2.35

Reducción al absurdo (*Reductio ad absurdum* (RAA, Abs)):

$$\begin{array}{l} \neg\phi \to \bot \\ \hline\hline \phi \end{array}$$

Observación 2.2.36.— Un caso de particular interés de RAA es cuando la fórmula ϕ es una implicación, por ejemplo $\phi \to \psi$, entonces su negación es $\phi \wedge \neg\psi$, por lo que, mediando la regla de intercambio, RAA queda

$$\begin{array}{l} \phi \wedge \neg\psi \to \bot \\ \hline\hline \phi \to \psi \end{array}$$

esto es,

- que $\phi \wedge \neg\psi$ implique una fórmula insatisfactible equivale a que ϕ implique ψ.

Notemos que, entonces, por contrapositiva, $\neg((\phi \wedge \neg\psi) \to \bot) \dashv\vdash \neg(\phi \to \psi)$; en otras palabras,

- que $\phi \wedge \neg\psi$ no implique una fórmula insatisfactible equivale a que ϕ no implique ψ,

y esto a $\phi \wedge \neg\psi$ (principio de CRISIPO). Aunque para este último viaje no hacían falta alforjas, esto no es más que un caso particular de la fórmula válida $\neg(\phi \to \bot) \to \phi$.

Ejemplo 126

Sean $P(x)$ y $Q(x)$ dos funciones proposicionales. En un universo consistente U (no existen contradicciones en él) donde sucede $\neg P(x) \vee Q(x)$ sabemos que $P(a)$ es verdadera, donde a es una entidad de U. ¿Es verdadera $Q(a)$ en U?

Resolución.— Como en U sucede $\neg P(x) \vee Q(x)$, en particular, $\neg P(a) \vee Q(a)$. Comencemos la RAA, si suponemos $\neg Q(a)$, entonces por IC, $(\neg P(a) \vee Q(a)) \wedge \neg Q(a)$, que por distributiva de $\wedge$ en $\vee$ (DisC), es $\neg P(a) \wedge \neg Q(a)$, lo que implica $\neg P(a) \vee \neg Q(a)$, ahora, por RES,
$$\frac{\begin{array}{l}\neg P(a) \vee Q(a)\\ \neg P(a) \vee \neg Q(a)\end{array}}{\neg P(a) \vee \neg P(a)}$$
en definitiva, $\neg P(a)$. Por lo que por IC, se satisface $P(a) \wedge \neg P(a)$ en U lo cual es imposible, por lo que por RAA no se satisface $\neg Q(a)$ sino $Q(a)$. ■

Principios constructivos, de sumación, destructivos y de consenso

Teorema 2.36 (Principios constructivos, I)

Principio constructivo (PCons_0):
$$\frac{\begin{array}{l}\phi \to \chi\\ \psi \to \chi\end{array}}{\phi \vee \psi \to \chi}$$
(double line)

(PCons_1):
$$\frac{\begin{array}{l}\phi \to \psi\\ \phi \to \chi\end{array}}{\phi \to \psi \wedge \chi}$$
(double line)

Teorema 2.37 (Principios constructivos, II)

Principio constructivo (PCons_2):
$$\frac{\begin{array}{l}\phi \to \psi\\ \chi \to \tau\end{array}}{\phi \vee \chi \to \psi \vee \tau}$$

(PCons_3):
$$\frac{\begin{array}{l}\phi \to \psi\\ \chi \to \tau\end{array}}{\phi \wedge \chi \to \psi \wedge \tau}$$

Teorema 2.38 (Principios de sumación)

Principio de sumación ($PSum_0$): $$\frac{\phi \to \psi}{\phi \vee \chi \to \psi \vee \chi}$$

($PSum_1$): $$\frac{\phi \to \psi}{\phi \wedge \chi \to \psi \wedge \chi}$$

($PSum_2$): $$\frac{\phi \to \psi}{(\psi \to \chi) \to (\phi \to \chi)}$$

Teorema 2.39 (Principios destructivos)

Principio destructivo ($PDes_0$): $$\frac{\phi \to \psi \qquad \chi \to \tau}{\neg\psi \vee \neg\tau \to \neg\phi \vee \neg\chi}$$

($PDes_1$): $$\frac{\phi \to \psi \qquad \chi \to \tau}{\neg\psi \wedge \neg\tau \to \neg\phi \wedge \neg\chi}$$

Teorema 2.40 (Consenso, I)

Regla de consenso (RCon): $$\frac{(\phi \wedge \psi) \vee (\neg\phi \wedge \chi) \vee (\psi \wedge \chi)}{(\phi \wedge \psi) \vee (\neg\phi \wedge \chi)}$$ (doble línea)

Teorema 2.41 (Consenso, II)

Dual de la regla de consenso (RCon′): $$\frac{\phi \vee \psi \qquad \neg\phi \vee \chi \qquad \psi \vee \chi}{(\phi \vee \psi) \wedge (\neg\phi \vee \chi)}$$ (doble línea)

Observación 2.2.37.— Se conoce como *consenso* (o, sinónimamente, *término de consenso*) a $\psi \wedge \chi$ en RCon y a $\psi \vee \chi$ en su dual RCon′.

Observación 2.2.38.— El caso particular de que ψ sea $\top$ recibe el nombre de *ley de consenso*[37]:

[37] *Cfr. supra* ejemplo 112 (pág. 172 de esta edición) para una demostración indirecta de LCon (allí se demuestra $p \vee q \leftrightarrow p \vee (\neg p \wedge q)$).

- puesto que $\phi \vee (\neg\phi \wedge \chi) \vee \chi$ equivale a $\phi \vee (\neg\phi \wedge \chi)$ y ésta equivale a $\phi \vee \chi$, de RCon tenemos:

Ley de consenso (LCon): $$\frac{\phi \vee (\neg\phi \wedge \chi)}{\phi \vee \chi}$$

- puesto que $\phi \wedge (\neg\phi \vee \chi) \wedge \chi$ equivale a $\phi \wedge (\neg\phi \vee \chi)$ y ésta equivale a $\phi \wedge \chi$, de RCon′ tenemos:

Dual de la ley de consenso (LCon′): $$\frac{\begin{matrix}\phi \\ \neg\phi \vee \chi\end{matrix}}{\phi \wedge \chi}$$

Reglas de interdefinición

Al ser $\{\neg, \wedge\}$, $\{\neg, \vee\}$ y $\{\neg, \rightarrow\}$ bases de juntores, es posible la definición mutua entre juntores. Destacamos también estas reglas.

Teorema 2.42 (Interdefiniciones de $\vee$ y $\wedge$)

Definición de $\wedge$ a partir de $\neg$ y $\vee$ (DC_0): $$\frac{\phi \wedge \psi}{\neg(\neg\phi \vee \neg\psi)}$$

Definición de $\vee$ a partir de $\neg$ y $\wedge$ (DD_0)
(Dual de DC_0, que pudiese designarse por $DC_0{}'$): $$\frac{\phi \vee \psi}{\neg(\neg\phi \wedge \neg\psi)}$$

Teorema 2.43 (Leyes de De Morgan)

Distribución de $\neg$ en $\vee$ (DM_0): $$\frac{\neg(\phi \vee \psi)}{\neg\phi \wedge \neg\psi}$$

Distribución de $\neg$ en $\wedge$ (DM_1)
(Dual de DM_0, que pudiese designarse por $DM_0{}'$): $$\frac{\neg(\phi \wedge \psi)}{\neg\phi \vee \neg\psi}$$

Teorema 2.44 (Interdefiniciones de $\vee$ y $\rightarrow$)

Definición de $\rightarrow$ a partir de $\neg$ y $\vee$ (DI_0): $$\frac{\phi \rightarrow \psi}{\neg\phi \vee \psi}$$

Definición de $\vee$ a partir de $\neg$ y $\rightarrow$ (DD_1): $$\frac{\phi \vee \psi}{\neg\phi \rightarrow \psi}$$

Teorema 2.45 (Interdefiniciones de ∧ y →)

Definición de → a partir de ¬ y ∧ (DI_1):

$$\frac{\phi \to \psi}{\neg(\phi \land \neg\psi)}$$

Definición de ∧ a partir de ¬ y → (DC_1):

$$\frac{\phi \land \psi}{\neg(\phi \to \neg\psi)}$$

Observación 2.2.39.— En este punto seremos conscientes de las múltiples presentaciones que puede tener una relación metalógica entre fórmulas, en particular, las reglas que estamos estudiando.

Por ejemplo, la regla deductiva doble DI_1 puede presentarse de manera equivalente por

Negación del implicador (NI):

$$\frac{\neg(\phi \to \psi)}{\phi \land \neg\psi}$$

que se corresponde con la equivalencia lógica ya estudiada, $\neg(\phi \to \psi) \equiv \phi \land \neg\psi$ (principio de Crisipo) y con la regla semántica *falsedad de la implicación* (FI)[38].

Reglas de reducción

Se conocen como *reglas de reducción* a las definiciones de los juntores habituales, ya en la base de juntores $\{\neg, \downarrow\}$, ya en la base $\{\neg, |\}$.

Teorema 2.46 (Reducción de la disyunción)

Reducción de ∨ a $\{\neg, \downarrow\}$ ($RedD_0$):

$$\frac{\phi \lor \psi}{\neg(\phi \downarrow \psi)}$$

Reducción de ∨ a $\{\neg, |\}$ ($RedD_1$):

$$\frac{\phi \lor \psi}{\neg\phi \mid \neg\psi}$$

[38] *Vid. infra* § 3.3.0 (págs. 275ss. de esta edición) y § 366 (págs. 381ss. de esta edición).

Ejemplo 127

De la afirmación «Tú lo haces o yo lo hago o lo hacemos ambas», nos preguntamos:
0.º, ¿qué afirmación se deduce de ella por RedD_0?, y
1.º, ¿qué afirmación se deduce de ella por RedD_1?
Comprobemos también en cada caso que de las deducidas, se deduce la original.

Resolución.— En efecto, de la afirmación «Tú lo haces o yo lo hago o lo hacemos ambas»:

0.º, se deduce la afirmación «Es falso que ni tú lo hagas ni yo lo haga» [por RedD_0] y recíprocamente, de esta última, la primera [también por RedD_0 al ser una regla doble], y

1.º, se deduce la afirmación «Que tú no lo hagas es incompatible con que yo no lo haga» [por RedD_1] y recíprocamente, de esta última, la primera [también por RedD_1 al ser una regla doble]. ■

Teorema 2.47 (Reducción de la conjunción)

Reducción de $\land$ a $\{\neg, \downarrow\}$ (RedC_0):
$$\frac{\phi \land \psi}{\neg\phi \downarrow \neg\psi}$$

Reducción de $\land$ a $\{\neg, \mid\}$ (RedC_1):
$$\frac{\phi \land \psi}{\neg(\phi \mid \psi)}$$

Ejemplo 128

De la afirmación «Tú lo haces y yo lo hago», nos preguntamos:
0.º, ¿qué afirmación se deduce de ella por RedC_0?, y
1.º, ¿qué afirmación se deduce de ella por RedC_1?
Comprobemos también en cada caso que de las deducidas, se deduce la original.

Resolución.— En efecto, de la afirmación «Tú lo haces y yo lo hago»:

0.º, se deduce la afirmación «Ni tú lo haces ni yo lo hago» [por RedC_0] y recíprocamente, de esta última, la primera [también por RedC_0 al ser una regla doble], y

1.º, se deduce la afirmación «Que tú lo hagas no es incompatible con que yo lo haga» [por RedC_1] y recíprocamente, de esta última, la primera [también por RedC_1 al ser una regla doble]. ■

Teorema 2.48 (Reducción de la implicación)

Reducción de $\to$ a $\{\neg, \downarrow\}$ (RedI_0):
$$\frac{\phi \to \psi}{\neg(\neg\phi \downarrow \psi)}$$

Reducción de $\to$ a $\{\neg, \mid$ (RedI_1):
$$\frac{\phi \to \psi}{\phi \mid \neg\psi}$$

Ejemplo 129

De la afirmación «Si tú lo haces, yo lo hago», nos preguntamos:
0.º, ¿qué afirmación se deduce de ella por RedI_0?, y
1.º, ¿qué afirmación se deduce de ella por RedI_1?
Comprobemos también en cada caso que de las deducidas, se deduce la original.

Resolución.— En efecto, de la afirmación «Si tú lo haces, yo lo hago»:

0.º, se deduce la afirmación «No es cierto que ni tú no lo haces ni yo lo hago» [por RedI_0] y recíprocamente, de esta última, la primera [también por RedI_0 al ser una regla doble], y

1.º, se deduce la afirmación «Que tú lo hagas es incompatible con que yo no lo haga» [por RedI_1] y recíprocamente, de esta última, la primera [también por RedI_1 al ser una regla doble]. ■

Teorema 2.49 (Reducción de la equivalencia)

Reducción de $\leftrightarrow$ a $\{\neg, \downarrow\}$:
$$\frac{\phi \leftrightarrow \psi}{(\neg\phi \downarrow \psi) \downarrow (\phi \downarrow \neg\psi)}$$

Reducción de $\leftrightarrow$ a $\{\neg, \mid\}$:
$$\frac{\phi \leftrightarrow \psi}{(\phi \mid \neg\psi) \mid (\neg\phi \mid \neg\psi)}$$

Ejemplo 130

De la afirmación «Tú lo haces si, y sólo si, yo lo hago», nos preguntamos:
0.º, ¿qué afirmación se deduce de ella por RedCO_0?, y
1.º, ¿qué afirmación se deduce de ella por RedCO_1?
Comprobemos también en cada caso que de las deducidas, se deduce la original.

Resolución.— En efecto, de la afirmación «Tú lo haces si, y sólo si, yo lo hago»:

0.°, se deduce la afirmación «No es cierto que ni tú no lo haces ni yo lo hago» [por RedCO_0] y recíprocamente, de esta última, la primera [también por RedCO_0 al ser una regla doble], y

1.°, se deduce la afirmación «Son incompatibles las siguientes dos afirmaciones: 0.ª, que tú lo hagas es incompatible con que yo no lo haga, y 1.ª, que tú no lo hagas es incompatible con que yo no lo haga» [por RedCO_1] y recíprocamente, de esta última, la primera [también por RedCO_1 al ser una regla doble]. ■

Observación 2.2.40.— Existen textos donde aparecen las reglas de reducción de la equivalencia como las siguientes:

Reducción (alternativa) de $\leftrightarrow$ a $\{\neg, \vee, \downarrow\}$ ($\mathrm{RedAltCO}_0$):
$$\frac{\phi \leftrightarrow \psi}{\neg((\neg\phi \downarrow \psi) \vee (\phi \downarrow \neg\psi))}$$

Reducción (alternativa) de $\leftrightarrow$ a $\{\neg, \wedge, |\}$ ($\mathrm{RedAltCO}_1$):
$$\frac{\phi \leftrightarrow \psi}{(\phi \mid \neg\psi) \wedge (\neg\phi \mid \psi)}$$

Ejemplo 131

De la afirmación «Tú lo haces si, y sólo si, yo lo hago», nos preguntamos:
0.°, ¿qué afirmación se deduce de ella por $\mathrm{RedAltCO}_0$?, y
1.°, ¿qué afirmación se deduce de ella por $\mathrm{RedAltCO}_1$?
Comprobemos también en cada caso que de las deducidas, se deduce la original.

Resolución.— En efecto, de la afirmación «Tú lo haces si, y sólo si, yo lo hago»:

0.°, se deduce la afirmación «Es falso afirmar que ni tú no lo haces ni yo lo hago o ni tú lo haces ni yo no lo hago, o ambas cosas» [por $\mathrm{RedAltCO}_0$] y recíprocamente, de esta última, la primera [también por $\mathrm{RedAltCO}_0$ al ser una regla doble], y

1.°, se deduce la afirmación «Suceden a la vez dos cosas: 0.ª, que tú lo hagas es incompatible con que yo no lo haga, y 1.ª, que tú no lo hagas es incompatible con que yo lo haga» [por $\mathrm{RedAltCO}_1$] y recíprocamente, de esta última, la primera [también por $\mathrm{RedAltCO}_1$ al ser una regla doble]. ■

Observación 2.2.41.— Recordemos que las reglas de interdefinición para la disyunción opuesta $\downarrow$ y la conjunción opuesta $|$ se muestran análogas a las leyes de De Morgan

Análoga a la ley de De Morgan DM_0 (OpDM_0):
$$\frac{\phi \downarrow \psi}{\neg(\neg\phi \mid \neg\psi)}$$

Análoga a la ley de De Morgan DM_1 (OpDM_1):
$$\frac{\phi \mid \psi}{\neg(\neg\phi \downarrow \neg\psi)}$$

Ejemplo 132

De las afirmaciones «Ni tú lo haces ni yo lo hago» y «Es incompatible que tú lo hagas con que yo lo haga», nos preguntamos:
0.º, ¿qué afirmación se deduce de la primera por OpDM_0?, y
1.º, ¿qué afirmación se deduce de la segunda por OpDM_1?
Comprobemos también en cada caso que de las deducidas, se deducen las originales.

Resolución.— En efecto:

0.º, de la afirmación «Ni tú lo haces ni yo lo hago» se deduce la afirmación «Es falso afirmar que tú no lo hagas sea incompatible con que yo no lo haga» [por OpDM_0] y recíprocamente, de esta última, la primera [también por OpDM_0 al ser una regla doble];

1.º, de la afirmación «Es incompatible que tú lo hagas con que yo lo haga» se deduce la afirmación «Es falso afirmar que ni tú no lo haces ni yo no lo hago» [por OpDM_1] y recíprocamente, de esta última, la primera [también por OpDM_1 al ser una regla doble]. ■

§ 2.3 Muestra de más ejemplos

Llegado el momento de poner en práctica lo aprendido: 0.º, comencemos por la conclusión, veamos si es equivalente a alguna fórmula más sencilla de derivar desde las premisas, e investiguemos supuestos que pudiesen cancelarse; 1.º, analicemos las premisas y con la conclusión en mente, intuyamos posibles asunciones posteriores que debiésemos hacer; 2.º, seamos conscientes de que algunas de las vías que exploremos pudiesen abocar en callejones sin salida.

§ 2.3.0 Derivación formal

Ejemplo 133

Utilicemos derivación formal para resolver la siguiente argumentación (ya resuelta por tablas de verdad en el ejemplo 93 [pág. 125 de esta edición]).

«Si el programa de cooperación en la sostenibilidad para el desarrollo (PCSD) no se frustra, entonces el PCSD debe comenzar y terminar. El PCSD comenzó y se frustró. Por lo tanto, el PCSD no terminó».

Resolución.— Recordemos que una formalización posible es:

$f \risingdotseq$ el PCSD se frustra;

$c \leftrightharpoons$ el PCSD comienza;

$t \leftrightharpoons$ el PCSD termina.

Se trata, pues, de encontrar una deducción formal de $\neg a$ desde $\{\neg f \to c \wedge t, e \wedge f\}$. Veamos.

0.	$\neg f \to c \wedge t$	[DF0] Premisa
1.	$c \wedge f$	[DF0] Premisa
2.	$c \wedge t \to t$	[DF1] EC_1
3.	$\neg f \to t$	[DF2] TrI 0, 2
4.	f	[DF2] EC_1 1
5.	$\neg t$	[?]

¿Será posible deducir $\neg a$ de las anteriores? No se nos ocurre cómo. Lo único que quiere decir esto es que no hemos sido capaces de encontrar una deducción formal, lo cual no indica que no la haya.

Lo que debemos hacer en casos como éste es aplicar otra estrategia. Lo hemos intentado en la sintaxis. Ahora bien, debido a que la lógica de juntores es correcta y completa[39], es posible hacerlo, bien desde la sintaxis, bien desde la semántica.

Preguntarnos en la sintaxis si $(\neg f \to c \wedge t) \wedge c \wedge f \to \neg t$ es un teorema lógico, esto es, si $\vdash (\neg f \to c \wedge t) \wedge c \wedge f \to \neg t$, equivale a preguntarnos en la semántica si es una fórmula válida, es decir, si $\vDash (\neg f \to c \wedge t) \wedge c \wedge f \to \neg t$.

Para resolver esta última cuestión, hallemos, por ejemplo, la tabla de verdad de $(\neg f \to c \wedge t) \wedge e \wedge f \to \neg t$. Justo esto lo hicimos en el ejemplo 93 (pág. 125 de esta edición). De allí observamos que la fórmula es contingente, y por tanto, obtenemos que $(\neg f \to c \wedge t) \wedge c \wedge f \to \neg t$ no es una fórmula válida y, de nuevo, por ser la lógica de juntores correcta y completa, que $(\neg f \to c \wedge t) \wedge c \wedge f \to \neg t$ no es un teorema lógico. En definitiva, la argumentación no es válida. ■

Ejemplo 134

¿Es válida la siguiente argumentación?

«Si echo una mano o soy persona de gran bonhomía, me sentiré satisfecha. Si me siento satisfecha, tendré paz interior. Como no tengo paz interior, esto significa que no eché una mano».

[Cubit 24].

Resolución.— Éste es el ejemplo 111 (pág. 168 de esta edición).

[39] *Vid. infra* teorema 6.9 (pág. 446 de esta edición).

Recordemos que una formalización posible es:

$p \leftrightharpoons$ echo una mano,

$q \leftrightharpoons$ soy persona de gran bonhomía,

$r \leftrightharpoons$ me siento satisfecha,

$s \leftrightharpoons$ tengo paz interior,

Vías 0, 1 y 2.

Abordaje directo (semántico).

En aquella ocasión apuntamos varias vías semánticas para su resolución. Pudiésemos decir que aquél constituyó el abordaje directo (semántico). En efecto, desde la semántica se trataría de averiguar si $\{p \vee q \to r, r \to s, \neg s\} \vDash \neg p$, tarea que por el teorema 1.14 (pág. 148 de esta edición) equivale a averiguar si $\vDash (p \vee q \to r) \wedge (r \to s) \wedge \neg s \to \neg p$, para lo que, por ejemplo, bastaría que hiciésemos su tabla de verdad, comprobando que de hecho se trata de una fórmula válida. Ésta fue la que llamamos vía 0. Las vías 1 y 2 vistas allí consistieron en su demostración por deducción semántica. □

Vía 3.

Abordaje indirecto (sintáctico).

Por ser la lógica de juntores correcta —teorema de corrección de Post[40]—, para demostrar $\vDash (p \vee q \to r) \wedge (r \to s) \wedge \neg s \to \neg p$, basta demostrar $\{p \vee q \to r, r \to s, \neg s\} \vdash \neg p$.

Así, desde la sintaxis, se trataría de averiguar si se deduce/deriva formalmente $\neg p$ del conjunto de fórmulas $\{p \vee q \to r, r \to s, \neg s\}$. Todo consistiría, pues, en encontrar una deducción formal, como así va a ocurrir. Para ello utilizamos las reglas[41] $DF0$, $DF1$ y $DF2$ para construir la siguiente derivación formal.

0.	$p \vee q \to r$	[DF0] Premisa
1.	$r \to s$	[DF0] Premisa
2.	$\neg s$	[DF0] Premisa
3.	$p \to p \vee q$	[DF1] ID_0
4.	$p \to r$	[DF2] Sil 3, 0
5.	$p \to s$	[DF2] Sil 4, 1
6.	$\neg p$	[DF2] MT 5, 2

donde ID es la regla de introducción del disyuntor, Sil es la ley del silogismo hipotético (transitiva del implicador) y MT es *modus tollens*. □

[40] *Vid. infra* el teorema 6.9 (pág. 446 de esta edición).
[41] *Vid. supra* definición 2.2 (pág. 182 de esta edición).

Vía 4.

Abordaje indirecto (sintáctico).

Una deducción formal alternativa, esta vez con supuesto y su cancelación es la siguiente:

0.	$(p \vee q) \to r$	[DF0] Premisa
1.	$r \to s$	[DF0] Premisa
2.	$\neg s$	[DF0] Premisa
3.	$\neg(p \vee q) \vee r$	DI_0 0
4.	r	Supuesto
5.	s	MP 1, 4
6.	$s \wedge \neg s$	IC 5, 2
7.	$\neg r$	RAA 4–6
8.	$\neg(p \vee q)$	MT 0, 7
9.	$\neg p \wedge \neg q$	DM_0 8
10.	$\neg p$	EC_0 9

donde DI es la regla definición del implicador (principio de FILÓN), MP es *modus ponens*, IC es la regla de introducción del conjuntor, RAA es la regla de reducción al absurdo, MT es *modus tollens*, DM es la ley de DE MORGAN y EC es la regla de eliminación del conjuntor. ■

Observación 2.3.0.— Observemos que en el abordaje indirecto —sintáctico— hemos pasado de la semántica a la sintaxis y vuelto a la semántica. Así, para una cuestión semántica, la demostración que hemos hecho ha sido exclusivamente sintáctica. Sólo un apunte, igual que en la traducción y traducción inversa entre lenguajes, debiésemos verificar las traslaciones entre ambos campos lingüísticos.

§ 2.3.1 Reducción al absurdo

Ejemplo 135

Utilicemos reducción al absurdo (Abs, RAA) para resolver la siguiente argumentación.

«Las IA (inteligencias artificiales) manejan creencias, pero una multitud de IA no es caótica, sino que está organizada colectivamente. De hecho, si una multitud de IA se organiza colectivamente y no es caótica, es porque las IA manejan creencias. Por tanto, puede concluirse que una multitud de IA no se organizará colectivamente siempre que no haya IA que manejen creencias».

[EFO 3.6.2019:1], [EFO 3.6.2019:1b2] (por reducción al absurdo).

Resolución.—

0. *Argumento* ($\mathcal{A}$): Las IA manejan creencias y una multitud de IA no es caótica y una multitud de IA se organiza colectivamente. Si las IA manejan creencias, entonces una multitud de IA se organiza colectivamente y no es caótica. Luego, si las IA no manejan crencias, entonces una multitud de IA no se organiza colectivamente.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

   - *Variables proposicionales*.

     Considerando como universo de discurso el conjunto de todas las IA, sean las siguientes tres variables proposicionales y sus correspondientes enunciados o proposiciones simples

     $p \coloneqq$ Las IA manejan creencias;

     $q \coloneqq$ Una multitud de IA es caótica;

     $r \coloneqq$ Una multitud de IA se organiza colectivamente.

   - *Esquema argumental*:

     Se tiene p y no q y r.
     Si se supone p, se sigue r y no q.

     $\therefore$ Se sigue que si se supone no p, se sigue no r.

   - *Forma lógica*.

Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{p \wedge \neg q \wedge r, p \rightarrow (r \wedge \neg q)\}$ y la conclusión ψ, a saber, $\neg p \rightarrow \neg r$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(p \wedge \neg q \wedge r) \wedge (p \rightarrow (r \wedge \neg q)) \rightarrow (\neg p \rightarrow \neg r)$. Llamémosla A.

2. *Resolución del argumento por reducción al absurdo*.

Utilicemos reducción al absurdo para demostrar que la proposición A es una fórmula válida y, por lo tanto, que el argumento $\mathcal{A}$ es válido.

Al suponer falso el implicador, la única posibilidad es que el antecedente, $(p \wedge \neg q \wedge r) \wedge (p \rightarrow (r \wedge \neg q))$, sea verdadero y el consecuente, $\neg p \rightarrow \neg r$, falso. De esto último, se tiene que $\neg p$ es verdadero y $\neg r$ falso; en otras palabras, p es falso y r es verdadero. Por otro lado, por ser el antecedente verdadero, la conjunción es verdadera y cada uno de los conjuntos, $p \wedge \neg q \wedge r$ y $p \rightarrow (r \wedge \neg q)$, también. Sin embargo, por ser p falso, el primer conjunto también lo es. Por tanto, el primer conjunto, $p \wedge \neg q \wedge r$ es verdadero y falso, a la vez, lo cual en la lógica de juntores bivalente no es posible; dicho de otro modo, hemos llegado a una fórmula insatisfactible. En resumen, de suponer $\neg A$ hemos deducido una fórmula insatisfactible, por lo que, de RAA se sigue que A es una fórmula válida; en otras palabras, el argumento $\mathcal{A}$ es válido e, igualmente, la argumentación es válida. ■

Observación 2.3.1.— En el ejemplo anterior, hemos identificado la estructura de $\mathcal{A}$ con ser $\phi_0 \wedge \phi_1 \rightarrow \psi$ una fórmula válida. Por el teorema 1.2 (pág. 71 de esta edición) sabemos que w es un contramodelo para dicha fórmula si, y sólo si, w es un modelo para Γ, donde $\Gamma = \{\phi_0, \phi_1\} \cup \{\neg\psi\} = \{p \wedge \neg q \wedge r, p \rightarrow (r \wedge \neg q), \neg(\neg p \rightarrow \neg r)\}$.

Ante una fuerte sospecha de que la argumentación sea válida, estudiamos si existe una refutación para Γ, en este caso por reducción al absurdo.

Como vimos en el apartado 2.III del ejemplo 93 (pág. 125 de esta edición) —en aquél caso para tablas de verdad—, debido al teorema 1.2 (pág. 71 de esta edición), es posible abordar directamente Γ, esto es, $(p \wedge \neg q \wedge r) \wedge (p \rightarrow (r \wedge \neg q)) \wedge \neg(\neg p \rightarrow \neg r)$, a partir de su verdad (*cfr.* 2.III.A de dicho ejemplo) o, equivalentemente, abordar $(p \wedge \neg q \wedge r) \wedge (p \rightarrow (r \wedge \neg q)) \rightarrow (\neg p \rightarrow \neg r)$, a partir de su falsedad (*cfr.* 2.III.B de dicho ejemplo).

Recordemos que esto se debe a que $\phi \wedge \neg\psi \equiv \neg(\phi \rightarrow \psi)$ (ley de Crisipo), que proporciona la vista de RAA como la regla[42] $\phi \wedge \neg\psi \rightarrow \bot \dashv\vdash \phi \rightarrow \psi$.

Estudiamos éste y los ejemplos siguientes tomando como punto de comienzo la falsedad de $(p \wedge \neg q \wedge r) \wedge (p \rightarrow (r \wedge \neg q)) \rightarrow (\neg p \rightarrow \neg r)$, esto es, la verdad de su negación, $\neg((p \wedge \neg q \wedge r) \wedge (p \rightarrow (r \wedge \neg q)) \rightarrow (\neg p \rightarrow \neg r))$, lo cual no es más que la verdad de su antecedente $(p \wedge \neg q \wedge r) \wedge (p \rightarrow (r \wedge \neg q))$ y la falsedad de su consecuente $\neg p \rightarrow \neg r$.

[42] *Cfr. supra* observación 2.2.36 (pág. 214 de esta edición).

Observación 2.3.2.— Más adelante, resolveremos este ejemplo mediante árboles semánticos[43].

Ejemplo 136

Utilicemos reducción al absurdo (Abs, RAA) para resolver la siguiente argumentación.

«Las personas colaboran cuando cooperan, pero no es cierto que cooperen si colaboran. Que las personas cooperen significa que se apoyan mutuamente. En definitiva, las personas se apoyan mutuamente siempre que cooperan aunque no colaboren».

[EFE 25.6.2019:1a], [EFE 25.6.2019:1b2] (por reducción al absurdo).

Resolución.—

0. *Argumento.*

- *Reescritura de la argumentación.*

  Identificamos tres oraciones enunciativas:

  I. «las personas que cooperan, colaboran, pero las que colaboran no tienen por qué cooperar» ($\mathcal{O}_1$), en la que identificamos «las personas que cooperan, colaboran» ($\mathcal{O}_{1a}$) y «las [personas] que colaboran no tienen por qué cooperar» ($\mathcal{O}_{1b}$) unidas por la conjunción adversativa «pero» ($\mathcal{O}_{1a}$ y $\mathcal{O}_{1b}$); en $\mathcal{O}_1$ está presente una elipsis del condicional material por lo que es posible reescribir $\mathcal{O}_{1a}$ como «si las personas cooperan, entonces las personas colaboran»; por otro lado, es posible reescribir $\mathcal{O}_{1b}$ como «no es cierto que las personas que colaboran, cooperen» o «colaborar no es suficiente para cooperar» y así, reescribimos $\mathcal{O}_{1b}$ como «es falso que si las personas colaboran, entonces las personas cooperan»;

  II. «que las personas cooperen significa que se apoyan mutuamente» ($\mathcal{O}_2$), estructura semántica que en nuestra lengua natural involucra un concepto sinonímico «p significa r» (como si encontrásemos r como definición de p en un diccionario); así, es posible reescribir $\mathcal{O}_2$, por ejemplo, como «afirmar que las personas cooperan es tanto como afirmar que las personas se apoyan mutuamente»;

  III. «las personas se apoyan mutuamente siempre que cooperan aunque no colaboren» ($\mathcal{O}_{3b}$), en la que identificamos «[las personas] cooperan aunque no colaboren» ($\mathcal{O}_{3b}$) formula una condición suficiente para que se cumpla que «las personas se apoyen mutuamente» ($\mathcal{O}_{3a}$), en otras palabras, que «si $\mathcal{O}_{3b}$, entonces $\mathcal{O}_{3a}$»; así, es posible reescribir $\mathcal{O}_3$ como «las personas que cooperan, tanto si colaboran como si no, se apoyan mutuamente».

---

[43] *Cfr. infra* ejemplo 155 (pág. 287 de esta edición).

- *Argumento* ($\mathcal{A}$): Si las personas cooperan, entonces las personas colaboran y es falso que si las personas colaboran, entonces las personas cooperan. Afirmar que las personas cooperan es tanto como afirmar que las personas se apoyan mutuamente. Luego, las personas que cooperan, tanto si colaboran como si no, se apoyan mutuamente.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

- *Variables proposicionales*:

  Considerando como universo de discurso el conjunto de todas las personas, sean las siguientes tres variables proposicionales y sus correspondientes enunciados o proposiciones simples:

$$p \eqqcolon \text{«Las personas cooperan»},$$
$$q \eqqcolon \text{«Las personas colaboran»},$$
$$r \eqqcolon \text{«Las personas se apoyan mutuamente»}.$$

- *Estructura lógico-gramatical*.

  Vista parcialmente a la hora de reescribir la argumentación. Con las variables anteriores, formalizamos en el lenguaje de la lógica de juntores, lo concluido allí en I, II y III, respectivamente, por: I, $(p \to q) \wedge \neg (q \to p)$ (ya que expresamos $\mathcal{O}_{1a}$ por $p \to q$ y $\mathcal{O}_{1b}$ por $\neg (q \to p)$); II, $p \leftrightarrow r$, y III, $(p \wedge (q \vee \neg q)) \to r$, que puede simplificarse a $p \to r$ al ser $\top$ [$q \vee \neg q$ es una fórmula válida] el elemento neutro de la conjunción.

- *Esquema argumental*:

  Si se supone p, se sigue q y es falso que si se supone q, se sigue p.
  Si se supone p, se sigue q, y recíprocamente.
  ___
  ∴ Se sigue que si se supone p, se sigue r.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{((p \to q) \wedge \neg (q \to p)), (p \leftrightarrow r)\}$ y la conclusión ψ, a saber, $p \to r$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(p \to q) \wedge \neg(q \to p) \wedge (p \leftrightarrow r) \to (p \to r)$. Llamémosla A.

2. *Resolución del argumento por reducción al absurdo*.

Utilicemos reducción al absurdo para demostrar que la proposición A es una fórmula válida y, por tanto, que el argumento $\mathcal{A}$ es válido.

Al suponer falso el implicador, la única posibilidad es que sea verdadero el antecedente, $((p \to q) \land \neg (q \to p)) \land (p \leftrightarrow r)$, y falso el consecuente, $(p \to r)$. De esto último, se tiene que p es verdadero y r es falso.

Por otro lado, por ser el antecedente verdadero, la conjunción es verdadera y cada uno de los conjuntos, $(p \to q)$, $\neg (q \to p)$ y $(p \leftrightarrow r)$, también. La veracidad del tercer conjunto implica que p y r tienen el mismo valor de verdad, en contra de lo deducido en el párrafo anterior. Dicho de otro modo, hemos llegado a una fórmula insatisfactible. En resumen, de suponer $\neg A$ hemos deducido una fórmula insatisfactible, por lo que, por reducción al absurdo, se tiene que A es una fórmula válida; en otras palabras, el argumento $\mathcal{A}$ es válido e, igualmente, la argumentación es válida. ■

Actividad 2.3

Elaboremos para este ejemplo una discusión en torno a Γ similar a la hecha en la observación 2.3.1 (pág. 227 de esta edición).

Observación 2.3.3.— Más adelante, resolveremos este ejemplo mediante árboles semánticos[44].

Ejemplo 137

Para resolver la siguiente argumentación, una vez formalizada, empleemos reducción al absurdo de tres maneras: utilizando una tabla de verdad como estrategia de verificación, utilizando una tabla de verdad como estrategia de refutación y utilizando derivación formal como estrategia de verificación.

«Sabemos que Cala viene siempre que viene Abigail. También sabemos que Cala viene si viene Balbina. Y nos han dicho que es seguro que una de las dos, Abigail o Balbina, va a venir. Así que también es seguro que Cala vendrá».

[EFE 29.6.2018:1a], [EFE 29.6.2018:1b1].

Resolución.—

0. *Argumento.*

 - *Reescritura de la argumentación.*

 Comencemos reescribiendo la argumentación para intentar aclarar su significado además de para acercarla a patrones más sencillos de traducción de los conectores de la lógica de juntores, identificando las premisas y la conclusión.

[44] *Cfr. infra* ejemplo 156 (pág. 289 de esta edición).

[Premisa 1] Si Abigail viene, entonces Cala viene.
[Premisa 2] Si Balbina viene, entonces Cala viene.
[Premisa 3] Abigail viene o Balbina viene o ambas vienen.
Así que,
[Conclusión] Cala viene.

- *Argumento* ($\mathcal{A}$): Si Abigail viene, entonces Cala viene. Si Balbina viene, entonces Cala viene. Abigail viene o Balbina viene o ambas vienen. Luego, Cala viene.

- *Validez intuitiva*.

  Intuitivamente se asemeja válido, pues de la tercera premisa debe suceder alguno de los disyuntos, que Abigail viene o que Balbina viene; si sucede el primero, de la primera premisa se tiene la conclusión; si sucede el segundo, de la segunda premisa se tiene la conclusión.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

- *Variables proposicionales*.

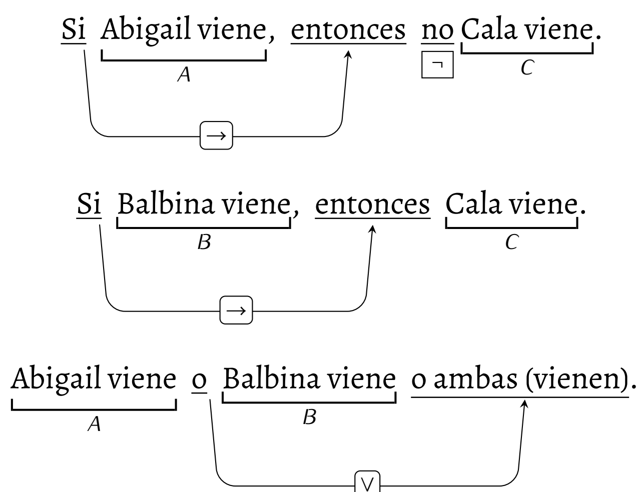
  Siendo el universo de discurso el conjunto de todas las personas, sean éstas las variables proposicionales y las proposiciones simples que representan (tomándonos la licencia de designar a aquéllas como a éstas, con letras latinas mayúsculas):

$$A \leftrightharpoons \text{Abigail viene}; \qquad B \leftrightharpoons \text{Balbina viene}; \qquad C \leftrightharpoons \text{Cala viene.}$$

- *Estructura lógico-gramatical*.

  Identificamos tres oraciones declarativas y la estructura deductiva $\{\mathcal{O}_0, \mathcal{O}_1, \mathcal{O}_2\} \vDash \mathcal{O}_3$, puesto que la conclusión ($\mathcal{O}_3$) está precedida de «Así que», un indicador de conclusión, esto es, apuntando a que la oración que sigue es la conclusión de las que la preceden.

  Subrayemos ahora los juntores e identifiquemos las proposiciones simples con las variables proposicionales que las representan.



$$\underbrace{\underline{\text{Así que,}}}_{\boxed{\therefore}}$$

$$\underbrace{\text{Cala viene}}_{C}.$$

Observemos que el indicador de conclusión «Así que» queda designado por la conectiva $\therefore$ del metalenguaje.

- *Esquema argumental*:

$$\begin{array}{ll} & \text{Si se supone } A\text{, se sigue } C. \\ & \text{Si se supone } B\text{, se sigue } C. \\ & \text{Se tiene } A \vee B. \\ \hline \therefore & \text{Se sigue } C. \end{array}$$

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2\} = \{A \to C, B \to C, A \vee B\}$, con una única premisa, y la conclusión ψ, a saber, C. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(A \to B) \wedge (B \to C) \wedge (A \vee B) \to C$. Llamémosla A.

2. *Resolución del argumento por reducción al absurdo*.

Como sabemos, el razonamiento por reducción al absurdo consiste en demostrar que un argumento $\mathcal{A}$ es válido, razonando a partir de suponer que no lo es, concretamente

$$(\neg\mathcal{A} \vdash 0) \vdash \mathcal{A}.$$

En su traducción al lenguaje de la lógica de juntores, si un argumento tiene la forma $P \to Q$, lo anterior queda:

$$(\neg(P \to Q) \to 0) \to (P \to Q),$$

que equivale a

$$(\neg(\neg P \vee Q) \to 0) \to (P \to Q),$$

y esta a

$$((P \wedge \neg Q) \to 0) \to (P \to Q),$$

que significa que si admitiendo simultáneamente la premisa y la negación de la conclusión, llegamos a una fórmula insatisfactible, entonces el argumento es válido.

En el caso de estudio, la premisa P es $(A \to C) \wedge (B \to C) \wedge (A \vee B)$ y la conclusión Q es C.

Por motivo pedagógico, mostramos tres vías.

Vía 0.

Mediante una tabla de verdad como estrategia de verificación,

A	B	C	((A	→	C)	∧(((B	→	C)	∧(A	∨	B))	∧	¬	C))	→	⊥
1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	0	1	1	0
1	1	0	1	0	0	0	1	0	0	0	1	1	1	0	1	0	1	0
1	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	1	0
1	0	0	1	0	0	0	0	1	0	1	1	1	0	1	1	0	1	0
0	1	1	0	1	1	0	1	1	1	1	0	1	1	0	0	1	1	0
0	1	0	0	1	0	0	1	0	0	0	0	1	1	0	1	0	1	0
0	0	1	0	1	1	0	0	1	1	0	0	0	0	0	0	1	1	0
0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1	0

conseguimos demostrar que, en efecto, la conjunción de las premisas y la negación de la conclusión conduce a contradicción. □

Vía 1.

Mediante una tabla de verdad como estrategia de refutación,

$((A$	$\to$	$C)$	$\land($	B	$\to$	$C)$	$\land($	A	$\lor$	$B))$	$\to$	C
0	1	0	1	0	1	0	1	0	1	0	0	0
4.°	3.°	2.°	1.°	6.°	3.°	2.°	1.°	5.°	3.°	7.°	0.°	1.°

donde los pasos han sido: 0.°, negación del argumento; 1.°, definición del implicador; 2.°, propagación del valor de verdad de C; 3.°, definición del conjuntor; 4.°, definición del implicador; 5.°, propagación del valor de verdad de A; 6.°, definición del implicador; 7.°, propagación del valor de verdad de B.

Observamos que hemos encontrado la fórmula insatisfactible $(A \lor B) \land \neg(A \lor B)$. □

Vía 2.

Mediante una derivación formal como estrategia de verificación, en la que partiendo de admitir simultáneamente la premisa y la negación de la conclusión, llegamos a $\bot$:

0.	$(A \to C) \land (B \to C) \land (A \lor B) \land \neg C$	[Antecedente de RAA]
1.	$(A \to C)$	[EC 0]
2.	$(B \to C)$	[EC 0]
3.	$(A \lor B)$	[EC 0]
4.	$\neg C$	[EC 0]
5.	$\neg A$	[MT 1, 4]
6.	$\neg B$	[MT 2, 4]
7.	B	[ED 3, 5]
8.	$\neg B \land B$	[IC 6, 7]
9.	$\bot$	[PC 8]

Observación.— Los acrónimos utilizados corresponden a las reglas deductivas: EC $\leftrightharpoons$ Eliminación del conjuntor; ED $\leftrightharpoons$ Eliminación del disyuntor; IC $\leftrightharpoons$ Introducción del conjuntor; MT $\leftrightharpoons$ *modus tollendo tollens*; PC $\leftrightharpoons$ principio de contradicción. ■

Observación 2.3.4.— Más adelante, resolveremos este ejemplo mediante árboles semánticos[45].

§ 2.3.2 De la isla de las personas veraces y falaces

Para pensar sobre los ejemplos siguientes y las ocho primeras actividades propuestas subsiguientes, *consideremos una isla donde todas las personas que la habitan son, o bien veraces, o bien falaces*. Una persona *veraz* es aquélla que siempre dice la verdad y *falaz* quien siempre miente. Si bien estos problemas tienen su origen en GARDNER [83], fueron popularizados por SMULLYAN, quien hablaba de *knights and knaves* en [84]. Esos nombres han sido traducidos al español también como las parejas (caballeros, bribones/escuderos/truhanes), (honestos/sinceros, mentirosos) y («veros», «mentos»).

Las actividades 2.7, 2.8 y 2.9 (págs. 249, 249 y 249 de esta edición) y los ejemplos 138, 139, 140, 141 y 142 (págs. 234, 238, 239, 241 y 245 de esta edición) proceden de SMULLYAN [85]; el ejemplo 143 (pág. 246 de esta edición) que procede de ZHÚKOV, SAMOVOL y APPLEBAUM [86].

Nos proponemos la resolución de las cuestiones aquí agrupadas como parte del entrenamiento del buen manejo de las reglas del sistema de deducción natural. Claro que también es un buen ejercicio mental aplicar tanto las diferentes estrategias estudiadas hasta este momento como las que están aún por conocer. Es por esto que debiésemos volver aquí durante el estudio futuro.

Lo habitual a la hora de resolver cuestiones de personas veraces y falaces es designar X para representar el hecho de ser X una persona veraz (por lo que $\neg X$ designa el hecho de ser X falaz) y S_X para representar lo que dice la persona X. Además, para toda persona X, se satisface $X \leftrightarrow S_X$ (de sencilla demostración, por haber sólo dos tipos de personas en la isla: si X es una persona veraz, entonces S_X, lo que dice X, es verdad; recíprocamente, si S_X, lo que dice X, es verdad, necesariamente X es una persona veraz). En resumen: $X \leftrightharpoons X$ es veraz; $\neg X \leftrightharpoons X$ es falaz; $S_X \leftrightharpoons$ (lo que dice X); $X \leftrightarrow S_X$ (la «regla básica»).

Ejemplo 138

Siendo A una de las personas que habita la isla, alguien le pregunta: «¿Es usted una persona veraz?»; A contesta: «Si soy una persona veraz, entonces, me comeré mi sombrero». Demostremos que A tiene que comerse su sombrero.

[Cubit 22], [SEL 2:1].

[45] *Cfr. infra* ejemplo 164 (pág. 312 de esta edición).

Resolución.— Sean:

$A \fallingdotseq$ A es una persona veraz;

$H \fallingdotseq$ A se come su sombrero.

Entonces, de $A \leftrightarrow S_A$ y $S_A \leftrightarrow (A \to H)$, por la transitividad de $\leftrightarrow$, tenemos $A \leftrightarrow (A \to H)$; ésta es nuestra premisa.

Resolvamos esta situación por dos vías.

Vía 0.

Simplifiquemos la expresión mediante una secuencia de equivalencias (a la KLEENE).

$A \leftrightarrow (A \to H)$	
$\equiv A \leftrightarrow (\neg A \vee H)$	[Principio de FILÓN]
$\equiv (A \wedge (\neg A \vee H)) \vee (\neg A \wedge \neg(\neg A \vee H))$	$(\phi \leftrightarrow \psi) \equiv (\phi \wedge \psi) \vee (\neg\phi \wedge \neg\psi)$
$\equiv ((A \wedge \neg A) \vee (A \wedge H)) \vee (\neg A \wedge \neg(\neg A \vee H))$	[Distributiva de $\wedge$ en $\vee$]
$\equiv (\mathrm{F} \vee (A \wedge H)) \vee (\neg A \wedge \neg(\neg A \vee H))$	[Insatisfactibilidad]
$\equiv (A \wedge H) \vee (\neg A \wedge \neg(\neg A \vee H))$	[F neutro para $\vee$]
$\equiv (A \wedge H) \vee (\neg A \wedge (\neg\neg A \wedge \neg H))$	[DE MORGAN]
$\equiv (A \wedge H) \vee (\neg A \wedge (A \wedge \neg H))$	[Doble Negación]
$\equiv (A \wedge H) \vee ((\neg A \wedge A) \wedge \neg H)$	[Asociativa de $\wedge$]
$\equiv (A \wedge H) \vee (\mathrm{F} \wedge \neg H)$	[Insatisfactibilidad]
$\equiv (A \wedge H) \vee \mathrm{F}$	[F absorbente para $\wedge$]
$\equiv A \wedge H$	[F neutro para $\vee$]

Concluimos que A es veraz y se come su sombrero. □

Vía 1.

Alternativamente, deduzcamos (derivemos) formalmente la conclusión utilizando el Principio del Tercero Excluido:

0.	$A \leftrightarrow (A \rightarrow H)$	Premisa
1.	$A \vee \neg A$	PTE
2.	$\neg A$	Supuesto
3.	$(A \rightarrow H) \rightarrow A$	ECO_1 0
4.	$\neg(A \rightarrow H)$	MT 3, 2
5.	$A \wedge \neg H$	NI 4
6.	A	EC 5
7.	$A \wedge \neg A$	IC 6, 2
8.	A	RAA 2–7
9.	$A \rightarrow (A \rightarrow H)$	ECO_0 0
10.	$A \rightarrow H$	MP 9, 8
11.	H	MP 10, 8
12.	$A \wedge H$	IC 8, 11

Concluimos que A es veraz y se come su sombrero. ■

Observación 2.3.5.— El artefacto *Proof Checker*[46, 47] de Christian Gottschall reconoce las ocho reglas básicas del SDN de Gentzen y Jaśkowski, si bien con una sintaxis particular[48], aunque algo similar a la usada por Edward John Lemmon en su libro *Beginning Logic*[49]. Aparentemente, no reconoce reglas derivadas —de ahí que haya tenido que introducir la coimplicación vía su definición (por otra parte, A es una palabra reservada para aserto por lo que utilizo P en vez de A para la persona)—, por lo que resulta que al introducir la siguiente demostración en el artefacto, éste devuelve que no reconoce la regla →N (negación del implicador) correspondiente al principio de Crisipo —aunque sí que la utiliza Christian Gottschall en otro de sus artefactos (nombrándola →R), concretamente en *The theorem prover*[50]— (ni qué decir tiene que he probado con →R y tampoco funciona en el *Proof Checker*).

[46] *Vid.* https://www.erpelstolz.at/gateway/formular-uk-beweis.html.

[47] Encontramos un artefacto similar, con la ventaja de ser FLOSS (*Free/Libre and Open Source Software*) (con licencia GPL v3), en https://proof-checker.org/ (su código: https://github.com/grbruns/capstone-openLogic) (parte del *Open Logic Project* [https://openlogicproject.org/], que incluye textos de libre descarga [https://openlogicproject.org/download/]).

[48] *Vid.* https://www.erpelstolz.at/gateway/proof-syntax.html.

[49] *Vid. v. gr.* https://en.wikipedia.org/wiki/Suppes%E2%80%93Lemmon_notation.

[50] *Vid.* https://www.erpelstolz.at/gateway//prover.html (eligiendo «Prove the proposition» en «Task to be performed» en https://www.erpelstolz.at/gateway/formular-uk-zentral.html).

1	(1)	(P → (P → H)) ∧ ((P → H) → P)	A
2	(2)	P ∨ ¬P	A
3	(3)	¬P	A
1	(4)	(P → H) → P	1 ∧E
1,3	(5)	¬(P → H)	4,3 MTT
1,3	(6)	P ∧ ¬H	5 →N
1,3	(7)	P	6 ∧E
1,3,3	(8)	P ∧ ¬P	7,3 ∧I
1	(9)	P	3,8 RAA
1	(10)	P → (P →H)	1 ∧E
1,1	(11)	P →H	10,9 MPP
1,1,1,1	(12)	H	11,9 MPP
1,1,1,1	(13)	P ∧ H	9,12 ∧I

Actividad 2.4

Completemos esta demostración con las reglas básicas adecuadas y comprobémosla en el artefacto *Proof Checker* comentado.

Observación 2.3.6.— En realidad existe una variedad de *sistemas de ayuda a la demostración*[51]. Entre ellos están Isabelle[52], Rocq[53] (antes Coq), Agda[54] y Lean[55]. Bastante de moda están en estos días —entre 2025 y 2026— Aristotle[56] y Lean[55], una pareja de artefactos que funciona: si tenemos en mente un teorema y la idea de su demostración, Aristotle nos ayuda a su formalización en Lean, que nos permitirá asegurar que todo es válido —por ejemplo, utilizándolos, Enrique Barschkis[57] ha publicado el 21 de enero de 2026 (con sólo 17 años) la resolución del problema 347 de Erdős[58] (teoría de números) (logro ya recogido en el wiki de Terence Tao[59] dedicado a los problemas de Erdős[60])—.

51 *Vid. v. gr.* https://en.wikipedia.org/wiki/Proof_assistant.
52 *Vid.* https://isabelle.in.tum.de/.
53 *Vid.* https://rocq-prover.org/.
54 *Vid.* https://wiki.portal.chalmers.se/agda/pmwiki.php.
55 *Vid.* https://lean-lang.org/.
56 *Vid.* https://aristotle.harmonic.fun/.
57 *Vid.* https://ch.linkedin.com/in/enrbar?trk=public_post_reshare-text.
58 *Vid.* https://www.erdosproblems.com/forum/thread/347.
59 *Vid.* https://terrytao.wordpress.com/.
60 *Vid.* https://github.com/teorth/erdosproblems/wiki/AI-contributions-to-Erd%C5%91s-problems.

Ejemplo 139

Sean A y B dos habitantes de la isla.

0. A dice: «Si B es veraz, entonces soy falaz». ¿Qué son A y B, veraces o falaces?
1. Seguidamente, B dijo: «No crea a A; miente». Con esta nueva información, ¿pudiésemos determinar si A y B son personas veraces o falaces?

[EFO 1.6.2017:1], [SEL 2:4].

Resolución.—

0. Formalizamos la afirmación de A, «Si B es veraz, entonces soy falaz» por $B \to \neg A$ y el hecho de que A lo diga, por $A \leftrightarrow (B \to \neg A)$. A la vista de la tabla de verdad

A	B	A	$\boxed{\leftrightarrow}$	$(B$	$\to$	$\neg$	$A)$
1	1	1	0	1	0	0	1
1	0	1	1	0	1	0	1
0	1	0	0	1	1	1	0
0	0	0	0	0	1	1	0

el único modelo para $A \leftrightarrow (B \to A)$ es la interpretación I_{10}, por lo que tanto puede determinarse que A es una persona veraz y B falaz.

1. La afirmación de B, «No crea a A; miente», es equivalente a «A es una persona falaz», que formalizamos por $\neg A$ y el hecho de que B lo diga, por $B \leftrightarrow \neg A$, que viene a afirmar que A y B no pueden ser ambas veraces ni ambas falaces, lo que no nos aporta nada nuevo, como era de esperar al estar ya determinado. En efecto, a la vista de la tabla de verdad

A	B	$(A$	$\leftrightarrow$	$(B$	$\to$	$\neg$	$A))$	$\boxed{\wedge}$	$(B$	$\leftrightarrow$	$\neg$	$A)$
1	1	1	0	1	0	0	1	0	1	0	0	1
1	0	1	1	0	1	0	1	1	0	1	0	1
0	1	0	0	1	1	1	0	0	1	1	1	0
0	0	0	0	0	1	1	0	0	0	0	1	0

observamos que todo sigue igual, de nuevo interpretación I_{10} es el único modelo, ahora para $(A \leftrightarrow (B \to \neg A)) \wedge (B \leftrightarrow \neg A)$.

Solución.— En ambos supuestos, la conclusión es la misma, a saber, que A es una persona veraz y B falaz. ■

Ejemplo 140

Nos encontramos con dos personas A y B, habitantes de la isla, que nos dicenlo siguiente. A: Como mucho una de nosotras dos es una persona falaz si, y sólo si, yo soy una persona falaz. B: Exactamente una de nosotras es una persona falaz. En esta ocasión, ¿es A una persona veraz o falaz?, ¿y B?

[EFE 7.7.2021:1].

Resolución.—

0. *Reescritura simplificadora*.

Razonemos reescribiendo lo dicho por A y B para intentar aclarar su significado y acercarlo a patrones más sencillos de traducción a la lógica de juntores.

> A dice: Que no suceda que yo sea una persona falaz a la vez que B sea también una persona falaz es equivalente a que yo sea una persona falaz.
> B dice: Sucede que A es una persona veraz o que yo soy una persona veraz, pudiendo suceder ambas cosas, pero no ocurre que A y yo seamos personas veraces ambas.

1. *Formalización de la situación expuesta en lógica de juntores.*

- *Variables proposicionales*.

  Considerando como universo de discurso el conjunto de todos las personas, tenemos las siguientes dos variables proposicionales y sus correspondientes proposiciones simples:

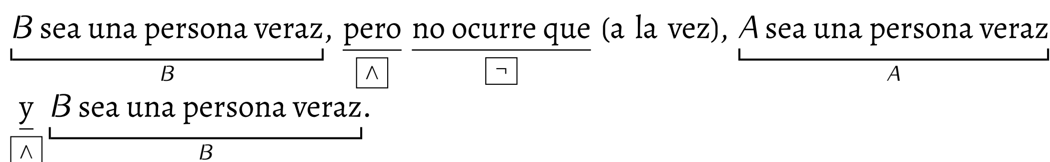
$$A : \text{«A es una persona veraz»},$$
$$B : \text{«B es una persona veraz»}.$$

- *Estructura lógico-gramatical*.

  Identificamos, pues, dos oraciones enunciativas, que notamos por S_A y S_B. Subrayemos ahora las conectivas e identifiquemos las proposiciones simples.

S_A: Que $\underset{\boxed{\neg}}{\underline{\text{no}}}$ suceda que, $\underset{\boxed{\neg}}{\underline{\text{no}}}$ suceda que $\underbrace{A \text{ sea una persona veraz}}_{A}$ $\underset{\boxed{\wedge}}{\underline{\text{a la vez que}}}$ $\underset{\boxed{\neg}}{\underline{\text{no}}}$ suceda que $\underbrace{B \text{ sea una persona veraz}}_{B}$, $\underset{\boxed{\leftrightarrow}}{\underline{\text{es equivalente a que}}}$ $\underset{\boxed{\neg}}{\underline{\text{no}}}$ suceda que $\underbrace{A \text{ sea una persona veraz}}_{A}$.

S_B: Sucede que $\underbrace{A \text{ sea una persona veraz}}_{A}$ $\underset{\boxed{\vee}}{\underline{\text{o (pudiendo suceder ambas cosas)}}}$ que



- *Forma lógica.*

  Expresado en lógica de juntores, lo que dice A es

$$S_A \leftrightharpoons \neg(\neg A \wedge \neg B) \leftrightarrow \neg A \tag{2.3}$$

y lo que dice B es

$$S_B \leftrightharpoons (A \vee B) \wedge \neg(A \wedge B), \tag{2.4}$$

que pueden expresarse con diversas fórmulas equivalentes, entre ellas, a modo de ejemplo:

$$\begin{aligned}
S_A &\leftrightharpoons \neg(\neg A \wedge \neg B) \leftrightarrow \neg A \\
&\equiv (A \vee B) \leftrightarrow \neg A && \text{(por ley de De Morgan)} \quad (2.5)\\
&\equiv (\neg A \to B) \leftrightarrow \neg A && \text{(por principio de Filón)}\\
&\equiv (\neg B \to A) \leftrightarrow \neg A && \text{(por contrarrecíproca de la implicación)}\\
S_B &\leftrightharpoons (A \vee B) \wedge \neg(A \wedge B)\\
&\equiv A \veebar B && \text{(definición de } \veebar) \quad (2.6)\\
&\equiv \neg A \veebar \neg B && \text{(definiciones de } \neg \text{ y } \veebar)\\
&\equiv \neg(\neg A \leftrightarrow \neg B) && \text{(definiciones de } \neg, \veebar \text{ y } \leftrightarrow)\\
&\equiv \neg(A \leftrightarrow B) \equiv \neg A \leftrightarrow B \equiv A \leftrightarrow \neg B && \text{(definiciones de } \neg \text{ y } \leftrightarrow) \quad (2.7)\\
&\equiv \neg((A \to B) \wedge (B \to A)) && \text{(definiciones de } \to \text{ y } \leftrightarrow)\\
&\equiv \neg(A \to B) \vee \neg(B \to A) && \text{(por ley de De Morgan)}\\
&\equiv (A \wedge \neg B) \vee (B \wedge \neg A) && \text{(por principio de Crisipo)}\\
&\equiv (\neg A \to B) \wedge (A \to \neg B) && \text{(de } \neg A \leftrightarrow B \text{ (2.7) y def. de } \to \text{ y } \leftrightarrow)
\end{aligned}$$

Utilizando que $X \leftrightarrow S_X$, la situación queda expresada por

$$(A \leftrightarrow S_A) \wedge (B \leftrightarrow S_B), \tag{2.8}$$

esto es, por ejemplo, sustituyendo (2.5) y (2.6) en (2.8), la situación expuesta en la cuestión queda expresada en lógica de juntores por

$$(A \leftrightarrow ((A \vee B) \leftrightarrow \neg A)) \wedge (B \leftrightarrow (A \veebar B)). \tag{2.9}$$

2. *Resolución de la situación.*

   Para obtener una conclusión, utilizamos *tablas de verdad como estrategia de verificación.*

Et voilà!

A	B	$(A \leftrightarrow ((A \vee B) \leftrightarrow \neg A)) \wedge (B \leftrightarrow (A \veebar B))$
1	1	1 0 1 1 1 0 0 1 0 1 0 1 0 1
1	0	1 0 1 1 0 0 0 1 0 0 0 1 1 0
0	1	0 0 0 1 1 1 1 0 0 1 1 0 1 1
[0]	[0]	0 1 0 0 0 0 1 0 [1] 0 1 0 0 0

Apreciamos cómo la tabla de verdad de (2.9) muestra cómo el único modelo es la interpretación I_{00}, lo que corresponde a que ambas personas, A y B, sean falaces.

Solución.— A y B son personas falaces. ■

Observación 2.3.7.— Es patente que los diferentes métodos aplicables de la lógica de juntores nos conducirían al mismo resultado. Por ejemplo, pudiésemos razonar utilizando reducción al absurdo (Abs, RAA):

- Si A fuese veraz, entonces S_A es verdad, en particular, $A \to \neg A \wedge \neg B$, de donde por *modus ponens*, $\neg A \wedge \neg B$, y por eliminación del $\wedge$, se tendría $\neg A$, esto es, A falaz; por tanto, A no puede ser veraz.
- Si B fuese veraz, entonces S_B es verdad, es decir, $\neg(A \leftrightarrow B)$, de donde como B es veraz, A es falaz, por lo que S_A no es verdad, esto es, $\neg((A \vee B) \leftrightarrow \neg A)$, de donde, $(A \vee B) \veebar \neg A$ y, como sucede $\neg A$, entonces $\neg(A \vee B)$, por lo que, por ley de De Morgan, $\neg A \wedge \neg B$ y, por tanto, por eliminación del $\wedge$, se tendría $\neg B$, esto es, B falaz; por tanto, B no puede ser veraz.

O por *equivalencias lógicas* o por cualquier otra estrategia que aprendamos.

En definitiva, tanto A como B son personas falaces.

Ejemplo 141

De acuerdo con este viejo problema, tres habitantes —A, B y C— estaban de pie en un jardín. Una cuarta persona, extranjera, D, que pasaba por allí le preguntó a A: «¿Es usted una persona veraz o falaz?». A respondió, pero algo confusamente, por lo que D no pudo entender lo que dijo A. Entonces D le preguntó a B: «¿Qué dijo A?». B respondió: «A dijo que es una persona falaz». A estas alturas, C dijo: «No crea usted a B; ¡está mintiendo!». La cuestión es: ¿qué son B y C?, ¿veraces?, ¿falaces?, ¿una veraz y la otra falaz?

[Cubit 28], [AIC 10.4.2018:1A], [EFE 22.6.2022:1], [SEL 2:2].

Resolución.—

1. *Formalización*.

0. *Formalización de la respuesta de B.*

Observamos que B habla de lo que dice otra persona, A. En este caso, si bien es factible aplicar la regla básica —la equivalencia entre lo que es B, veraz o falaz, y lo que dice B—, $B \leftrightarrow S_B$, nos preguntamos qué sucede con la relación de implicación y replicación entre S_B y lo que efectivamente dice B, ¿existe una relación bicondicional entre ellas? La realidad es que no, la relación no es de bicondicionalidad.

Designemos por «A dice . . .» lo que dice efectivamente B. La implicación $S_B \rightarrow$ «A dice . . .» sí es verdadera, ya que si lo que dice B es cierto, entonces es cierto que A dice lo que B dice que dice. Sin embargo, la implicación recíproca, «A dice . . .» $\rightarrow S_B$ no es verdadera, ya que si lo que dice B no es verdadero, entonces no tenemos ni idea de lo que dice A—observemos que admitir «A dice . . .» $\rightarrow S_B$ equivaldría a admitir $\neg S_B \rightarrow \neg$«$A$ dice . . .», y este es precisamente el quid de la cuestión, que de $\neg S_B$ es inviable deducir nada sobre lo que dice A—.

Así, tenemos, por una parte, $B \leftrightarrow S_B$ [por la regla básica] y, por otra, $S_B \rightarrow (A \leftrightarrow \neg A)$, por la explicación anterior junto a $A \leftrightarrow S_A$ [por la regla básica] y $S_A \leftrightarrow \neg A$ [es lo que dice B que dijo A]; como $A \leftrightarrow \neg A$ equivale a Falsum, entonces $S_B \rightarrow (A \leftrightarrow \neg A)$ equivale a $S_B \rightarrow$ Falsum, esto es, a $\neg S_B \vee$ Falsum, es decir, a $\neg S_B$.

Por todo esto, la respuesta de B, «A dijo que es una persona falaz», se formaliza por $(B \leftrightarrow S_B) \wedge (\neg S_B)$.

1. *Formalización de lo que dice C.*

Por otro lado, lo que dice C, «No crea usted a B; ¡está mintiendo!», esto es, simplemente, «B es una persona falaz», se formaliza $C \leftrightarrow \neg B$, a saber, $C \leftrightarrow S_C$ [por la regla básica] y $S_C \leftrightarrow \neg B$ [es lo que dice C], y por transitiva de $\leftrightarrow$, tenemos que lo que dice C se formaliza por $C \leftrightarrow \neg B$.

2. *Formalización de la situación expuesta en el enunciado.*

Así, la situación planteada se formaliza por $(B \leftrightarrow S_B) \wedge (\neg S_B) \wedge (C \leftrightarrow \neg B)$.

II. *Estrategia.*

Vía 0.

Pudiésemos simplificar la expresión mediante una secuencia de equivalencias (a la KLEENE) (*cfr.* actividad 2.5 [pág. 245 de esta edición]).

$$
\begin{aligned}
& (C \leftrightarrow \neg B) \wedge (B \leftrightarrow S_B) \wedge \neg S_B \\
\equiv\ & [\ldots] \\
\equiv\ & C \wedge \neg B \wedge \neg S_B
\end{aligned}
$$

Concluimos que C es veraz y B falaz y que A no dijo que fuese falaz.

De hecho, de ser B falaz se sigue que A no dijo que fuese una persona falaz, ya que al ser B falaz, lo que dice B no es verdad. □

Vía 1.

Deducción (derivación) formal utilizando el Principio del Tercero Excluido:

0.	$(C \leftrightarrow \neg B) \wedge (B \leftrightarrow S_B) \wedge \neg S_B$	Premisa
1.	$C \leftrightarrow \neg B$	EC 0
2.	$C \vee \neg C$	PTE
3.	$\neg C$	Supuesto
4.	$\neg B \to C$	ECO_1 1
5.	$\neg\neg B$	MT 4, 3
6.	B	DN 5
7.	$B \leftrightarrow S_B$	EC 0
8.	$B \to S_B$	ECO_0 7
9.	S_B	MP 8, 6
10.	$\neg S_B$	EC 0
11.	$S_B \wedge \neg S_B$	IC 9, 10
12.	C	RAA 3–11
13.	$C \to \neg B$	ECO_0 1
14.	$\neg B$	MP 13, 12
15.	$C \wedge \neg B$	IC 12, 14

En definitiva, hemos concluido que C es veraz y B falaz. □

Vía 2.

Deducción formal sin utilizar PTE[61]:

[61] A partir de una idea de Sara GUILLÉN TORRADO (año académico 2021-2022).

La forma normal disyuntiva de $C \leftrightarrow \neg B$ es $(B \wedge \neg C) \vee (\neg B \wedge C)$. En otras palabras, la respuesta es uno de los disyuntos o ambos.

El primer disyunto no puede suceder, pues si B fuese una persona veraz, entonces sería cierto que A dijo que era una persona falaz, pero ningún habitante de la isla puede hacer esa afirmación: una persona que siempre dice la verdad no puede afirmar que siempre miente y una persona que siempre miente tampoco puede afirmar que siempre miente.

Es posible demostrar que sucede el segundo disyunto, por ejemplo, mediante una derivación formal.

0.	$(B \leftrightarrow S_B) \wedge (\neg S_B) \wedge (C \leftrightarrow \neg B)$	[Premisa]
1.	$B \leftrightarrow S_B$	[EC 0]
2.	$\neg S_B$	[EC 0]
3.	$C \leftrightarrow \neg B$	[EC 0]
4.	$B \rightarrow S_B$	[ECO$_0$ 1]
5.	$\neg B$	[MT 4, 2]
6.	$\neg B \rightarrow C$	[ECO$_1$ 3]
7.	C	[MP 6, 5]
8.	$\neg B \wedge C$	[IC 5, 7]

Observación.— Los acrónimos utilizados corresponden a las siguientes reglas: EC = eliminación del conjuntor; ECO$_0$ = eliminación ($\rightarrow$) del coimplicador; ECO$_1$ = eliminación ($\leftarrow$) del coimplicador; MT = *modus tollendo tollens*; MP = *modus ponendo ponens*; IC = introducción del conjuntor.

III. *Conclusión.*— La estrategia diseñada e implementada nos ha servido para llegar a una conclusión, a saber, que únicamente sucede $\neg B \wedge C$.

Solución.— B es una persona falaz y C una persona veraz; por otro lado, A no dijo que fuese una persona falaz. ■

Observación 2.3.8.— Demostrar que sucede el segundo disyunto equivale a demostrar que $((B \leftrightarrow S_B) \wedge (\neg S_B) \wedge (C \leftrightarrow \neg B)) \rightarrow (\neg B \wedge C)$ es una fórmula válida. Para ello, pudiésemos haber utilizado cualquier otra estrategia como una tabla de verdad o una tabla semántica[62] (como una breve anticipación). Por ejemplo, puede realizarse su tabla de verdad con el artefacto en línea Wolfram|Alpha[63] con la entrada `(((B xnor S) and (not S)) and (C xnor (not B))) implies (not B and C)` y su tabla semántica en *The Truth Tree Solver*[64] con la entrada `(((B equiv S) and (not S)) and (C equiv (not B))) and not (not B and C)`.

[62] *Cfr. infra* § 3.3 (pág. 274 de esta edición).
[63] *Cfr.* https://www.wolframalpha.com/.
[64] *Cfr. infra* § 3.3.9 (pág. 319 de esta edición).

Actividad 2.5

Completemos y documentemos una demostración por equivalencias partiendo de $(C \leftrightarrow \neg B) \wedge (B \leftrightarrow S_B) \wedge \neg S_B$ y concluyendo $C \wedge \neg B \wedge \neg S_B$.

Ejemplo 142

Estaban tres personas A, B y C, lugareñas de la isla, de pie en el jardín delantero de una casa. Una persona foránea, que pasaba por allí, les preguntó: «¿Son ustedes personas veraces o falaces?»

0. A contestó: «Ninguna de nosotras es una persona falaz». ¿Pudiésemos determinar si A, B y C eran personas veraces o falaces?
1. Seguidamente, B dijo: «Como mucho, una de nosotras es una persona veraz». Con esta nueva información, ¿pudiésemos determinar si A, B y C eran personas veraces o falaces?

[EFE 7.7.2017:1].

Resolución.—

0. Utilizamos una tabla de verdad como estrategia de verificación.

A	B	C	A	$\boxed{\leftrightarrow}$	A	$\wedge$	$(B$	$\wedge$	$C)$
1	1	1	1	1	1	1	1	1	1
1	1	0	1	0	1	0	1	0	0
1	0	1	1	0	1	0	0	0	1
1	0	0	1	0	1	0	0	0	0
0	1	1	0	1	0	0	1	1	1
0	1	0	0	1	0	0	1	0	0
0	0	1	0	1	0	0	0	0	1
0	0	0	0	1	0	0	0	0	0

Interpretando los modelos, vemos que puede ocurrir: 0.º, que las tres sean personas veraces; 1.º, que A sea falaz y B y C veraz; 2.º, que A y C sean falaces y B veraz; 3.º, que A y B sean falaces y C veraz, o 4.º, que las tres sean personas falaces.

En definitiva, no tenemos nada concluyente.

1. Utilizamos de nuevo una tabla de verdad.

$A\ B\ C$	$(A \leftrightarrow A \wedge (B \wedge C))$ $\boxed{\wedge}$ $(B \leftrightarrow ((\neg A \wedge (\neg B \wedge \neg C)) \vee ((A \wedge (\neg B \wedge \neg C)) \vee ((\neg A \wedge (B \wedge \neg C)) \vee (\neg A \wedge (\neg B \wedge C))))))$
1 1 1	1 1 1 1 1 1 1 0 1 0 0 1 0 0 1 0 0 1 0 1 0 0 1 0 0 1 0 0 1 0 1 0 0 1 0 0 1 0 0 1 0 1
1 1 0	1 0 1 0 1 0 0 0 1 0 0 1 0 0 1 0 1 0 0 1 0 0 1 0 1 0 0 0 1 0 1 1 1 0 0 0 1 0 0 1 0 0
1 0 1	1 0 1 0 0 0 1 0 0 1 0 1 0 1 0 0 0 1 0 1 0 1 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 0 1 1
1 0 0	1 0 1 0 0 0 0 0 0 0 0 1 0 1 0 1 1 0 1 1 1 1 0 1 1 0 1 0 1 0 0 0 1 0 0 0 1 0 1 0 0 0
0 1 1	0 1 0 0 1 1 1 0 1 0 1 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 0 0 1 0 0 1 0 1 0 0 0 1 0 1
0 1 0	0 1 0 0 1 0 0 1 1 1 1 0 0 0 1 0 1 0 1 0 0 0 1 0 1 0 1 1 0 1 1 1 1 0 1 1 0 0 0 1 0 0
0 0 1	0 1 0 0 0 0 1 0 0 0 1 0 0 1 0 0 0 1 1 0 0 1 0 0 0 1 1 1 0 0 0 0 0 1 1 1 0 1 1 0 1 1
0 0 0	0 1 0 0 0 0 0 0 0 0 1 0 1 1 0 1 1 0 1 0 0 1 0 1 1 0 0 1 0 0 0 0 1 0 0 1 0 0 1 0 0 0

Sólo hay un modelo. Su interpretación es que A y C son personas falaces y B es veraz.

Utilizando la *disyunción exclusiva triádica*,

$$\veebar_3 ABC \leftrightharpoons (A \wedge (\neg B \wedge \neg C)) \vee (\neg A \wedge (B \wedge \neg C)) \vee (\neg A \wedge (\neg B \wedge C)),$$

la tabla de verdad es más sencilla:

$A\ B\ C$	$(A \leftrightarrow (A \wedge (B \wedge C)))$ $\boxed{\wedge}$ $(B \leftrightarrow ((\neg A \wedge (\neg B \wedge \neg C)) \vee (\veebar_3 A\ B\ C)))$
1 1 1	1 1 1 1 1 1 1 0 1 0 0 1 0 0 1 0 0 1 0 0 1 1 1
1 1 0	1 0 1 0 1 0 0 0 1 0 0 1 0 0 1 0 1 0 0 0 1 1 0
1 0 1	1 0 1 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 0 0 1 0 1
1 0 0	1 0 1 0 0 0 0 0 0 0 0 1 0 1 0 1 1 0 1 1 1 0 0
0 1 1	0 1 0 0 1 1 1 0 1 1 1 0 0 0 1 0 0 1 0 0 0 1 1
0 1 0	0 1 0 0 1 0 0 1 1 1 1 0 0 0 1 0 1 0 1 1 0 1 0
0 0 1	0 1 0 0 0 0 1 0 0 0 1 0 0 1 0 0 0 1 1 1 0 0 1
0 0 0	0 1 0 0 0 0 0 0 0 0 1 0 1 1 0 1 1 0 1 0 0 0 0

Solución.— En el primer caso, no llegamos a nada concluyente. En el segundo, A y C son personas falaces y B es veraz. ■

Actividad 2.6

En el ejemplo anterior, razonemos por qué S_A y S_B se formalizan, respectivamente, como $A \wedge B \wedge C$ y como $(\neg A \wedge (\neg B \wedge \neg C)) \vee (A \wedge (\neg B \wedge \neg C)) \vee (\neg A \wedge (B \wedge \neg C)) \vee (\neg A \wedge (\neg B \wedge C))$.

Ejemplo 143

Tres personas de dicha isla de sólo veraces y falaces dicen: la primera, «Sólo una de nosotras miente», la segunda, «Sólo una de nosotras nunca miente» y la tercera, «Ustedes mienten»; debemos averiguar qué tipo de habitante es cada una, si falaz o veraz.

[Cubit 25].

Resolución.— La deducción formal es la siguiente. Las premisas 0–2 provienen de considerar sólo personas veraces y falaces; las premisas 3–5 de lo que dicen tales personas. Las fórmulas en 6–8

son deducciones inmediatas de las premisas; TCO ⥦ transitiva del coimplicador. Las fórmulas en 9–10, 11–12 y 13–14 son deducciones inmediatas de las fórmulas en 6, 7 y 8, respectivamente; ECO ⥦ eliminación del coimplicador. En la situación en estudio, nos damos cuenta de que A y B no pueden decir la verdad a la vez; incorporamos sintácticamente esta realidad en 15, como una tautología. En 16 abrimos la discusión sobre C; PTE ⥦ principio del tercio excluso ($\phi \vee \neg\phi \dashv\vdash \top$). En 17–25 sucede la cancelación del supuesto C: los acrónimos son: MP ⥦ *modus ponens*; EC ⥦ eliminación del conjuntor; IC ⥦ introducción del conjuntor; ID ⥦ introducción del disyuntor; PC ⥦ principio de contradicción ($\phi \wedge \neg\phi \dashv\vdash \bot$). En 26 deducimos $\neg C$ por reducción al absurdo (RAA). En 27 abrimos la discusión sobre A, dado $\neg C$. En 28–43 sucede la cancelación de A, vía una prueba por casos (Cas —sinónimamente, eliminación del disyuntor (ED)—), B y $\neg B$, sucediendo la cancelación de B en 31–34 y la de $\neg B$ en 35–42. En 44 deducimos $\neg A$ por reducción al absurdo. En 45 abrimos la discusión sobre B, dados $\neg C$ y $\neg A$. En 46–50 sucede la cancelación de $\neg B$. En 51 deducimos B por reducción al absurdo. En 53 tenemos la conclusión, $\neg A \wedge B \wedge \neg C$.

0.	$A \leftrightarrow S_A$	Premisa
1.	$B \leftrightarrow S_B$	Premisa
2.	$C \leftrightarrow S_C$	Premisa
3.	$S_A \leftrightarrow (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$	Premisa
4.	$S_B \leftrightarrow (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$	Premisa
5.	$S_C \leftrightarrow \neg A \wedge \neg B$	Premisa
6.	$A \leftrightarrow (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$	TCO 0, 3
7.	$B \leftrightarrow (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$	TCO 1, 4
8.	$C \leftrightarrow \neg A \wedge \neg B$	TCO 2, 5
9.	$A \rightarrow (\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$	ECO_0 6
10.	$(\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C) \rightarrow A$	ECO_1 6
11.	$B \rightarrow (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$	ECO_0 7
12.	$(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C) \rightarrow B$	ECO_1 7
13.	$C \rightarrow \neg A \wedge \neg B$	ECO_0 8
14.	$\neg A \wedge \neg B \rightarrow C$	ECO_1 8
15.	$((\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)) \wedge$ $((A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)) \rightarrow \bot$	Tautología
16.	$C \vee \neg C$	PTE
17.	C	Supuesto
18.	$\neg A \wedge \neg B$	MP 13, 17
19.	$\neg B$	EC_1 18

20.	$\neg A \wedge \neg B \wedge C$	IC 18, 17
21.	$(\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$	ID 20
22.	$(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$	ID 21
23.	B	MP 22, 12
24.	$B \wedge \neg B$	IC 23, 19
25.	$\bot$	PC 24
26.	$\neg C$	RAA 17–25
27.	$A \vee \neg A$	PTE
28.	A	Supuesto
29.	$(\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)$	MP 9, 28
30.	$B \vee \neg B$	PTE
31.	B	Supuesto
32.	$(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$	MP 11, 31
33.	$((\neg A \wedge B \wedge C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge B \wedge \neg C)) \wedge$ $((A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C))$	IC 29, 32
34.	$\bot$	MP 15, 33
35.	$\neg B$	RAA 31–34
36.	$A \wedge \neg B$	IC 28, 35
37.	$A \wedge \neg B \wedge \neg C$	IC 36, 26
38.	$(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C)$	ID 37
39.	$(A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$	ID 38
40.	B	MP 12, 39
41.	$B \wedge \neg B$	IC 40, 35
42.	$\bot$	PC 41
43.	$\bot$	Cas 30, 31–34, 35–42
44.	$\neg A$	RAA 28–43
45.	$B \vee \neg B$	PTE
46.	$\neg B$	Supuesto
47.	$\neg A \wedge \neg B$	IC 44, 46
48.	C	MP 14, 47
49.	$C \wedge \neg C$	IC 48, 26
50.	$\bot$	PC 49
51.	B	RAA 46–50

52.	$\neg A \wedge B$	IC 44, 51
53.	$\neg A \wedge B \wedge \neg C$	IC 52, 26

Solución.— La segunda persona, B, es quien dice la verdad; la primera, A, y la tercera, C, mienten. ■

§ 2.4 Propuesta de más actividades

Como ya hemos comentado, las siguientes tres cuestiones proceden de SMULLYAN [85].

Actividad 2.7

Se rumorea que hay oro enterrado en la isla. Llegamos a ésta y le preguntamos a una de las personas que la habita, A, si hay oro en la isla. Nos responde como sigue: «Hay oro en esta isla si, y sólo si, yo soy una persona veraz». En éstas,

0. ¿es posible determinar si A es veraz o falaz?;
1. ¿es posible determinar si hay oro en la isla?

[SEL 2:5].

Con miras a su resolución.— $A \leftrightarrow (G \leftrightarrow A)$, donde $G \leftrightharpoons$ hay oro en la isla. *Sol.*— Hay oro en la isla pero A puede ser una persona veraz o falaz.

Actividad 2.8

(*Vid*. ejemplo 141 [pág. 241 de esta edición]). Supongamos que la persona extranjera, D, en vez de preguntar a A qué es, le preguntó a A: «¿Cuántas personas veraces hay entre ustedes?». De nuevo, A responde confusamente. Así que D le pregunta a B: «¿Qué dijo A?». B responde: «A dijo que hay una persona veraz entre nosotras». Entonces, C dice: «No crea usted a B; ¡está mintiendo!». Ahora, ¿qué son B y C?

[SEL 2:6].

Con miras a su resolución.— $(C \leftrightarrow \neg B) \wedge (B \leftrightarrow S_B) \wedge (S_B \rightarrow (A \leftrightarrow \top))$. *Sol.*— A no dijo que fuese una persona falaz, B es una persona falaz y C es una veraz.

Actividad 2.9

De nuevo, tenemos tres habitantes, A, B y C. A y B hacen las siguientes declaraciones:

A: Todas nosotras somos personas falaces.
B: Exactamente una es una persona veraz.
¿Qué son A, B y C?

[SEL 2:7].

Con miras a su resolución.— $(C \leftrightarrow (\neg A \land \neg B \land \neg C)) \land (B \leftrightarrow ((A \land \neg B \land \neg C) \lor (\neg A \land B \land \neg C) \lor (\neg A \land \neg B \land C)))$. *Sol.—* A y C son personas falaces y B es una persona veraz.

Las siguientes cuatro cuestiones, que completan este conjunto de diez sobre veraces y falaces (los dos últimos ejemplos y estas ocho primeras actividades), corresponden a la visita de McGregor (*vid.* SMULLYAN [87] (Parte 2: La lógica de mentir y de decir la verdad, § 3 El empadronador [págs. 25–28]): «Una vez, el empadronador señor McGregor realizó cierto trabajo de campo en la isla de las personas veraces y falaces. En esa visita McGregor decidió entrevistar solamente a las parejas».

Actividad 2.10

(Y). McGregor llamó a una puerta; una persona, digamos A, la abrió a medias y le preguntó a McGregor qué deseaba.
Hago un censo —respondió McGregor—, y necesito información sobre usted y su pareja. ¿Cuál, si alguien lo es, es una persona veraz, y cuál, si alguien lo es, es una persona falaz?
—¡Mi pareja y yo somos falaces!— dijo A con enojo mientras cerraba la puerta de un golpe.
¿Es A veraz?, ¿falaz?, ¿y la pareja de A?

[SEL 2:3].

Con miras a su resolución.— $A \leftrightarrow (\neg A \land \neg B)$ (siendo B la pareja de A). *Sol.—* A es una persona falaz y B una veraz.

Actividad 2.11

(O). En la casa siguiente, McGregor le preguntó a la persona, digamos A, que abrió la puerta, acerca de ella y su pareja:
—¿Son usted y su pareja, ambas, personas falaces?
A respondió: —Por lo menos una lo es.
¿Es A veraz?, ¿falaz?, ¿y la pareja de A?

[SEL 2:8].

Con miras a su resolución.— $A \leftrightarrow (\neg A \lor \neg B)$ (siendo B la pareja de A). *Sol.—* A es una persona veraz y B una falaz.

Actividad 2.12

(Si–entonces). La siguiente casa que visitó McGregor resultó un mayor enigma. Una persona, digamos A, algo introvertida, abrió la puerta tímidamente. Cuando McGregor le pidió que dijera algo sobre ella y su pareja, lo único que dijo A fue: —Si soy una persona veraz, entonces también lo es mi pareja. McGregor se fue no muy complacido. —¿Cómo puedo deducir algo sobre alguna persona de esta pareja a partir de una respuesta tan evasiva?— pensó. Estaba a punto de escribir, «Pareja, ambos componentes desconocidos», cuando recordó súbitamente una vieja lección de lógica de sus días de estudio en la universidad. Por supuesto —se dio cuenta—, puedo determinar de qué tipo es cada persona de la pareja. ¿Es A veraz?, ¿falaz?, ¿y la pareja de A?

[SEL 2:9].

Con miras a su resolución.— $A \leftrightarrow (A \rightarrow B)$ (siendo B la pareja de A). *Sol.*— A y B son personas veraces.

Actividad 2.13

(Si, y sólo si). Cuando McGregor entrevistó a la cuarta pareja, una de las personas, digamos A, dijo: —Mi pareja y yo somos personas del mismo tipo, o ambas somos veraces o ambas somos falaces.
(A podría haber dicho alternativamente: —Soy una persona veraz si, y sólo si, mi pareja es una persona veraz. Es lo mismo.)
¿Qué puede deducirse sobre A y qué puede deducirse sobre su pareja?

[SEL 2:10].

Con miras a su resolución.— $A \leftrightarrow (A \leftrightarrow B)$ (siendo B la pareja de A). *Sol.*— B es una persona veraz, pero A puede ser veraz o falaz.

Las tres cuestiones siguientes se basan en *El mercader de Venecia* de William SHAKESPEARE. En él, «Porcia tenía tres cofres: uno de oro, otro de plata y otro de plomo. Dentro de uno de estos cofres, Porcia había puesto su retrato y en cada uno había una inscripción. Porcia explicó a su pretendiente que cada inscripción podía ser, bien verdadera, bien falsa y que a partir de la inscripción debería averiguar qué cofre contenía el retrato. Si tenía éxito podría casarse con ella». *Vid.* BACKHOUSE [88] (págs. 49–52). El libro de SMULLYAN [85] contiene más versiones.

Actividad 2.14

(pág. 49) Supongamos entonces que Porcia tiene dos cofres, uno dorado y el otro plateado y que dentro de uno de ellos, depositó su retrato y sobre ellos escribió las inscripciones. Dorado: El retrato no está en éste. Plateado: Exactamente una de las dos inscripciones es verdadera. ¿Qué cofre debiese elegir quien la pretende?
Proporcionemos una demostración formal para nuestra respuesta. Usemos las siguientes abreviaturas: G: el retrato está en el cofre dorado; S: el retrato está en el cofre plateado; g: la inscripción del cofre dorado es verdadera; s: la inscripción del cofre plateado es verdadera.

[SEL 2:11].

Con miras a su resolución.— Una formalización de las premisas es la siguiente: el retrato está en uno, y sólo uno, de los cofres, $(G \wedge \neg S) \vee (S \wedge \neg G)$; inscripción del cofre dorado, $g \leftrightarrow \neg G$; inscripción del cofre plateado, $s \leftrightarrow ((g \wedge \neg s) \vee (s \wedge \neg g))$.

Actividad 2.15

(1.25) Supongamos que Porcia escribe la siguiente inscripción en los tres cofres: Dorado: El retrato está aquí. Plúmbeo: Al menos dos de las inscripciones de los cofres son falsas. ¿Qué cofre debiese elegir quien la pretende?
Proporcionemos un argumento informal y convincente en apoyo de nuestra respuesta. Usando las siguientes abreviaturas, establezcamos formalmente las premisas en las que se basa nuestro argumento: G: el retrato está en el cofre dorado; S: el retrato está en el cofre plateado; L: el retrato está en el cofre plúmbeo; g: la inscripción del cofre dorado es verdadera; s: la inscripción del cofre plateado es verdadera; l: la inscripción del cofre plúmbeo es verdadera.

[SEL 2:12].

Con miras a su resolución.— Una formalización de las premisas es la siguiente: el retrato está en uno, y sólo uno, de los cofres, $(G \wedge \neg S \wedge \neg L) \vee (\neg G \wedge S \wedge \neg L) \vee (\neg G \wedge \neg S \wedge L)$; inscripción del cofre dorado, $g \leftrightarrow G$; inscripción del cofre plateado, $s \leftrightarrow S$; inscripción del cofre plúmbeo, $l \leftrightarrow ((\neg g \wedge \neg s) \vee (\neg g \wedge \neg l) \vee (\neg s \wedge \neg l))$.

Actividad 2.16

(1.26) En esta versión del problema, Porcia introduce una daga en uno de los cofres. Quien la pretende debe elegir un cofre que no contenga la daga. Las inscripciones de los cofres son como sigue. Dorado: La daga está en este cofre. Plateado: La daga no está en este cofre. Plúmbeo: Como mucho una de las inscripciones de los cofres es verdadera.
De nuevo, debemos proporcionar un argumento informal y convincente para la correcta elección del cofre. Establezcamos formalmente también las premisas en las que se basa nuestro argumento. En esta ocasión usemos G, S o L, para indicar que la daga está en el cofre dorado, plateado o plúmbeo, respectivamente.

[SEL 2:13].

Con miras a su resolución.— Una formalización de las premisas es la siguiente: el retrato está en uno, y sólo uno, de los cofres, $(G \wedge \neg S \wedge \neg L) \vee (\neg G \wedge S \wedge \neg L) \vee (\neg G \wedge \neg S \wedge L)$; inscripción del cofre dorado, $g \leftrightarrow G$; inscripción del cofre plateado, $s \leftrightarrow \neg S$; inscripción del cofre plúmbeo, $l \leftrightarrow \neg((g \wedge s) \vee (g \wedge l) \vee (s \wedge l))$.

Para las dos siguientes, la estrategia de reducción al absurdo pudiese ayudar.

Actividad 2.17

Consideremos cien frases, la primera afirma que sólo una de las cien es falsa, la segunda que sólo dos de las cien son falsas, la tercera que sólo tres de las cien son falsas, y así sucesivamente hasta las dos últimas, la nonagésima novena que afirma que sólo noventa y nueve de las cien son falsas, y la centésima frase que afirma que las cien son falsas; ¿cuántas de estas cien frases son verdaderas?

[Cubit 26].

Con miras a su resolución.— Suponer verdadera la frase 100 lleva a contradicción (la propia frase 100 sería verdadera y falsa a la vez); luego, cancelamos dicho supuesto y, por reducción al absurdo, la frase 100 es falsa. Suponer verdadera la frase 99 es posible. Si suponemos verdadera la frase 98, habría 98 frases falsas y 2 verdaderas; delante de la 98 sólo puede haber 97 falsas, por lo que habría una falsa después, la 100, obligando [por tener que haber dos verdaderas] a que sea verdadera la 99, además de la 98 [el supuesto]; pero esto es una contradicción, a saber, «hay exactamente 98 frases falsas y hay exactamente 99 frases falsas»; luego, el supuesto se cancela y, por reducción al absurdo, la frase 98 es falsa. Si suponemos verdadera la frase 97, habría 97 frases falsas y 3 verdaderas; delante de la 97 sólo puede haber 96 falsas, por lo que habría una falsa después, la 100, obligando [por tener que haber tres verdaderas] a que sean verdaderas la 98 y la 99, además de la 97 [el supuesto]; pero esto es una contradicción, a saber, «hay exactamente 97 frases falsas y hay exactamente 98 frases falsas y hay exactamente 99 frases falsas»; luego, el supuesto se cancela y por reducción al absurdo, la frase 97 es falsa. Y así, sucesivamente, se van cancelando todos los supuestos (la frase 96 es verdadera, la frase 95 es verdadera, . . ., la frase 2 es verdadera, la frase 1 es verdadera), y por reducción al absurdo, las frases 96, 95, . . ., 2 y 1 son falsas, resultando que la única frase verdadera es la 99.

Actividad 2.18

Demostremos que en una colección de palabras binarias que satisfacen que en ninguna un 1 precede a un 0, si una de tales palabras comienza por 1, en ella no figura ningún 0.

[Cubit 27].

Con miras a su resolución.— Supongamos que hay una palabra cuya letra inicial es 1 (notemos este hecho por P) y su letra de lugar k es 0 (notemos este hecho por $\neg Q$), entonces, como 1 no puede preceder a 0, la letra de lugar $k-1$ es 0, por la misma razón, la letra de lugar $k-2$ es 0, y así sucesivamente, la letra inicial es 0; y ésta es precisamente la contradicción a la que llegamos, a saber, que la letra inicial de dicha palabra es 1 y 0, esto es, $P \wedge \neg Q \vdash \bot$; luego, por la tautología reducción al absurdo, tenemos $P \to Q$, esto es, si una palabra comienza por la letra 1, entonces la letra 0 no figura en ningún lugar en ella.

§ 2.5 Bibliografía

- Para una primera aproximación:

[62] María Manzano Arjona y Antonia Huertas Sánchez. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

[63] Pascual Casañ Muñoz y Amador Antón Antón. *Lógica matemática. Ejercicios. I. Lógica de enunciados*. NAU llibres, Valencia, España, 1991.

- Para estudiar y saber más:

[64] Manuel Garrido Giménez. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

[65] Carmen García Trevijano. *El arte de la lógica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1999.

- Para profundizar, acullá:

[66] Manuel Garrido Giménez, Luis Manuel Valdés Villanueva, Jesús Mosterín de las Heras, Alfonso García Suárez y Carlos-Peregrín Fernández Otero. *Lógica y lenguaje*. Cuadernos de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1989.

[67] Raymond Merrill Smullyan. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

[60] Herbert Bruce Enderton. *A mathematical introduction to logic*. Harcourt/Academic Press, San Diego, Condado de San Diego, California (US-CA), Estados Unidos de América, 2.ª ed., 2001.

Capítulo 3

De la semántica. II

Si no se sabe adonde se va, se corre el riesgo de encontrarse en otra parte.

(Robert Frank Mager).

La verdad, como el aceite, quedan encima siempre.

§ 3.0 Simplificación de una fórmula

Una primera cuestión es cómo reducir una fórmula a su forma equivalente más sencilla. Claro que quizás debiésemos reflexionar y discutir el significado preciso de esta relación «ser más sencilla que». Sencillez, ¿en cuanto a qué?, ¿a que los juntores participantes en la fórmula transformada sean de menor potencia que los que aparecen en la original?, ¿a que la fórmula transformada sea de menor longitud? En la literatura suele entenderse una combinación de ambas características y, salvo que ocasionalmente digamos lo contrario, así también lo haremos: sencillez en cuanto a juntores de menor potencia y expresión de menor longitud.

Ejemplo 144

¿Existe una expresión equivalente más simple de $(\neg\phi \vee \psi) \wedge (\phi \vee \neg\psi) \wedge (\phi \vee \psi)$?

Resolución.— Si hacemos la tabla de verdad,

ϕ	ψ	(($\neg$	ϕ	$\vee$	ψ)	$\wedge$	(ϕ	$\vee$	$\neg$	ψ))	$\boxed{\wedge}$	(ϕ	$\vee$	ψ)
1	1	0	1	1	1	1	1	1	0	1	1	1	1	1
1	0	0	1	0	0	0	1	1	1	0	0	1	1	0
0	1	1	0	1	1	0	0	0	0	1	0	0	1	1
0	0	1	0	1	0	1	0	1	1	0	0	0	0	0

observamos que es equivalente a $\phi \wedge \psi$. De hecho, pudiésemos aventurarnos a decir que ésta es una *expresión minimal* de la fórmula original. ■

Observación 3.0.0.— En este punto de nuestro estudio, no está de más conocer que, alternativamente a las tablas de verdad, es posible utilizar, por ejemplo, los *diagramas de* MARQUAND (1881), redescubiertos por VEITCH[0] (1952), los *mapas de* KARNAUGH[1] (1953), refinamiento de los anteriores, o el *algoritmo de* QUINE y MCCLUSKEY[2] desarrollado por QUINE (1952) y extendido por MCCLUSKEY (1956), funcionalmente idéntico a los mapas de KARNAUGH pero más eficiente de cara a su implementación computacional.[3]

Observación 3.0.1.— En el día a día de nuestros actos de comunicación, imaginemos que alguien ha utilizado un lenguaje enrevesado, pomposo o retórico, y que lo dicho tiene como fórmula correspondiente en la lógica de juntores $(\neg\phi \vee \psi) \wedge (\phi \vee \neg\psi) \wedge (\phi \vee \psi)$. ¿Por qué se expresó así cuando pudiese haber expresado lo mismo mucho más breve, clara y llanamente, $\phi \wedge \psi$?

En § 3.1.2 (pág. 260 de esta edición), estudiaremos una segunda cuestión, a saber, averiguar la fórmula correspondiente a una valoración dada conocido el número de variables proposicionales. Utilizaremos las formas normales para hacerlo por dos vías.

§ 3.1 Normalización: formas normales

Desde la semántica —teoría de modelos—, sería posible estudiar en este momento muchas más equivalencias, así como sus correspondientes fórmulas válidas, pero quizás sea mejor dejar para más

[0] *Vid. v. gr.* https://en.wikipedia.org/wiki/Edward_W._Veitch o BROWN [89] (págs. 42ss.).
[1] *Vid. v. gr.* https://es.wsustituciónikipedia.org/wiki/Mapa_de_Karnaugh.
[2] *Vid. v. gr.* https://es.wikipedia.org/wiki/Algoritmo_Quine-McCluskey.
[3] Para el estudio de los mapas de KARNAUGH y el algoritmo de QUINE y MCCLUSKEY, es posible interactuar con los artefactos en línea (https://www.uni-marburg.de/de/fb12/arbeitsgruppen/grafikmultimedia/lehre/ti de Thorsten THORMÄHLEN (https://www.uni-marburg.de/en/fb12/research-groups/grafikmultimedia/thormae).

adelante su presentación y hacerla desde la sintaxis —teoría de la demostración—, como reglas de inferencia y sus correspondientes teoremas lógicos.

No obstante, sí que estudiamos a continuación las formas normales, debido a su amplio interés como procedimiento de reducción a una estructura semántica común. Concretamente, se trata de reducir la fórmula original a otra que sólo contenga juntores de la base no minimal $\{\neg, \wedge, \vee\}$.

Aunque su exposición es desde la semántica, lo que se establece a continuación sobre formas normales tiene una expresión inmediata en la sintaxis como una estrategia de deducción más[4]. De hecho, así lo hemos aplicado para solucionar desde la sintaxis el ejemplo 133 (pág. 222 de esta edición).

Insistamos una vez más en que este desarrollo indistinto en la semántica y en la sintaxis sucede porque la lógica de juntores es correcta y completa[5]. Caso de presentar las formas normales desde la sintaxis, entonces, en el teorema 3.1 (pág. 263 de esta edición), las equivalencias lógicas ($\equiv$) serían sustituidas por reglas de inferencia deductivas dobles ($\dashv\vdash$), esto es, por teoremas[6] o por reglas de inferencia deductivas[7] (en la forma $\phi \vdash \psi$) y sus recíprocas (en la forma $\phi \dashv \psi$), que también serían, en dicho caso, teoremas o reglas de inferencia.

§ 3.1.0 Formas normales conjuntiva y disyuntiva

Definición 3.0.— Decimos que una fórmula está en *forma normal conjuntiva* (FNC) —o *forma normal clausal*— precisamente si tiene la forma

$$\phi \wedge \psi \wedge \chi \wedge \cdots$$

donde $\phi, \psi, \chi \ldots$ son literales o disyunciones de literales, esto es, si, y sólo si, es una conjunción de cláusulas[8].

Definición 3.1.— Decimos que una fórmula está en *forma normal disyuntiva* (FND) precisamente si tiene la forma

$$\phi \vee \psi \vee \chi \vee \cdots$$

donde $\phi, \psi, \chi \ldots$ son literales o conjunciones de literales, esto es, si, y sólo si, es una disyunción de cubos[8].

4 *Cfr. infra* § 6.0.2 (pág. 448 de esta edición).
5 *Vid. infra* teorema 6.9 (pág. 446 de esta edición).
6 *Vid. supra* definición 2.4 (pág. 185 de esta edición).
7 *Vid. supra* definición 2.0 (pág. 177 y ss. de esta edición).
8 Literales, cubos y cláusulas: *vid. supra* § 0.7.7 (pág. 57 de esta edición).

Ejemplo 145

Propongamos cuatro ejemplos de fórmulas que podamos interpretar como FNC y FND a la vez.

Resolución.— Por ejemplo, éstas:

0. p está en FNC, ya que es una cláusula, y en FND, pues es un cubo.
1. $\neg p$ está en FNC, pues es una cláusula, y en FND, ya que es un cubo.
2. $p \wedge q$ está en FNC, pues es una conjunción de dos cláusulas, y en FND, ya que es un cubo.
3. $p \vee q$ está en FNC, ya que es una cláusula, y en FND, pues es una disyunción de dos cubos. ■

§ 3.1.1 Formas normales completas, canónicas y mínimas

Definición 3.2.— Decimos que una fórmula ϕ está en *FND-completa* precisamente si cada una de sus variables aparece exactamente una vez en cada cubo. De cada uno de estos cubos decimos que es una *conjunción completa* respecto de la fórmula ϕ.

Definición 3.3.— Decimos que una fórmula ϕ está en *FNC-completa* precisamente si cada una de sus variables aparece exactamente una vez en cada cláusula. De cada una de estas cláusulas decimos que es una *disyunción completa* respecto de la fórmula ϕ.

Definición 3.4.— Decimos que una fórmula está en *forma normal disyuntiva canónica* precisamente si se expresa como

$$\bigvee_{I \in \mathfrak{I}} (\phi_I \wedge m_I),$$

donde ϕ_I es el valor de ϕ para la interpretación I y m_I es la conjunción completa correspondiente a la interpretación I.

Definición 3.5.— Decimos que una fórmula está en *forma normal conjuntiva canónica* precisamente si se expresa como

$$\bigwedge_{I \in \mathfrak{I}} (\phi_I \wedge \neg m_I),$$

donde ϕ_I es el valor de ϕ para la interpretación I y $\neg m_I$ es la disyunción completa, o sea, la negación de la conjunción completa, correspondiente a la interpretación I.

Observación 3.1.0.— En el ámbito de los sistemas digitales, es el *maxitérmino* (resp., el *minitérmino*) el que corresponde a la disyunción completa (resp., a la conjunción completa). Lo corres-

pondiente a la FND canónica (resp., FNC canónica) de una fórmula, es la representación de una función lógica como suma de minitérminos (resp., producto de maxitérminos).

Definición 3.6.— Decimos que una forma normal está en *forma mínima* si la expresión tiene el mínimo número posible de términos (cláusulas o cubos) y cada término tiene el mínimo número posible de literales.

Ejemplo 146

¿Cuál es la forma normal mínima de las siguientes fórmulas?

0. $(\neg p \wedge q \wedge r) \vee (p \wedge q \wedge r)$;
1. $(p \wedge q) \vee (p \wedge q \wedge r)$.

Resolución.—

0. La fórmula $(\neg p \wedge q \wedge r) \vee (p \wedge q \wedge r)$ está en forma normal disyuntiva canónica; su forma normal mínima, disyuntiva y conjuntiva, es $q \wedge r$.

1. La fórmula $(p \wedge q) \vee (p \wedge q \wedge r)$ está en forma normal disyuntiva; su forma normal mínima, disyuntiva y conjuntiva, es $p \wedge q$. ■

Observación 3.1.1.— Estudiemos de nuevo el ejemplo 144 (pág. 257 de esta edición).

Teorema 3.0

Toda fórmula puede reescribirse en forma normal disyuntiva y en forma normal conjuntiva.

Demostración.— Puede desarrollarse como la situación general de lo que estudiaremos a continuación en el ejemplo 147 (pág. 261 de esta edición). ■

§ 3.1.2 Normalización y el número total de juntores

Las definiciones de forma normal disyuntiva canónica y forma normal conjuntiva canónica nos permiten afirmar que la lógica de juntores no necesita de más juntores de los veinte ya estudiados, pues cualquier juntor enádico pudiese definirse a partir del conocimiento de su semántica; es decir, siempre es posible definir una fórmula a partir de los valores de verdad de sus interpretaciones (lo cual no es más que decir que una fórmula queda caracterizada por sus modelos, o equivalentemente, por sus contramodelos).

Veamos con un ejemplo cómo obtener las expresiones en FND canónica y en FNC canónica de un juntor desconocido a partir de su tabla de verdad.

Ejemplo 147

Imaginemos que la semántica de un juntor triádico, expresado en notación prefijo $*pqr$, viene dada por esta tabla de verdad.

p	q	r	$*pqr$	
1	1	1	0	($\leftarrow$-- vía 1)
1	1	0	0	($\leftarrow$-- vía 1)
1	0	1	1	($\leftarrow$-- vía 0)
1	0	0	1	($\leftarrow$-- vía 0)
0	1	1	0	($\leftarrow$-- vía 1)
0	1	0	1	($\leftarrow$-- vía 0)
0	0	1	0	($\leftarrow$-- vía 1)
0	0	0	1	($\leftarrow$-- vía 0)

Hallemos una fórmula de la lógica de juntores cuya tabla de verdad sea ésta. (Entenderemos el porqué de las anotaciones relativas a las vías al estudiar la resolución).

Resolución.— Las dos vías de razonamiento son las siguientes.

Vía 0.

Bastaría hacer la disyunción de los modelos para obtener una fórmula lógicamente equivalente a $*pqr$ en la base de juntores $\{\neg, \vee, \wedge\}$, esto es,

$$(p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge \neg r),$$

siendo ésta una expresión de $*pqr$ en forma normal disyuntiva, concretamente en la conocida como forma normal disyuntiva canónica. □

Vía 1.

Bastaría hacer la negación de la disyunción de los contramodelos para obtener una fórmula lógicamente equivalente a $*pqr$ en la base de juntores $\{\neg, \vee, \wedge\}$, esto es,

$$\neg\left((p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge r)\right),$$

que por las leyes de De Morgan es equivalente a

$$(\neg p \vee \neg q \vee \neg r) \wedge (\neg p \vee \neg q \vee r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee q \vee \neg r),$$

siendo ésta una expresión de $*pqr$ en forma normal conjuntiva, concretamente en la conocida como forma normal conjuntiva canónica. ■

Observación 3.1.2.— El artefacto en línea Normalform[9] calcula las expresiones en forma normal conjuntiva y en forma normal disyuntiva a partir de una tabla de verdad.

Observación 3.1.3.— En el ámbito de los sistemas digitales, dijésemos del ejemplo 147 (pág. 261 de esta edición) que nos han proporcionado la definición de una función lógica triádica mediante su tabla de verdad; en la vía 0 hemos representado dicha función como suma de los minitérminos, mientras que en la vía 1 la hemos representado como producto de los maxitérminos.

§ 3.1.3 Algoritmo de obtención de las formas normales de una fórmula dada

Si bien es posible obtener las formas normales canónicas a partir de la tabla de verdad como en el ejemplo 147 (pág. 261 de esta edición), dichas formas normales obedecen al patrón estricto de la canonicidad.

Si nuestro interés radica en encontrar la forma normal, conjuntiva o disjuntiva, de una fórmula dada (sin el requisito de canonicidad), entonces es oportuno aplicar el siguiente procedimiento, siempre teniendo presente que si en cualquier momento necesitásemos alguna otra equivalencia de las que aparecen a continuación, sería admisible utilizarla.

Suponemos que la fórmula está definida en la base $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$. Ahora bien, si participasen más juntores, en el paso FN0 eliminaríamos todos los que no fuesen de la base $\{\neg, \vee, \wedge\}$.

Paso 0 (FN0).
Eliminación de $\leftrightarrow$ y $\rightarrow$.

$$\begin{aligned} \phi \leftrightarrow \psi &\equiv \phi \rightarrow \psi \wedge \psi \rightarrow \phi; \\ \phi \rightarrow \psi &\equiv \neg\phi \vee \psi \\ &\equiv \neg(\phi \wedge \neg\psi). \end{aligned}$$

Paso 1 (FN1).
Interiorización de $\neg$.

$$\begin{aligned} \neg\neg\phi &\equiv \phi; \\ \neg(\phi \wedge \psi) &\equiv \neg\phi \vee \neg\psi; \\ \neg(\phi \vee \psi) &\equiv \neg\phi \wedge \neg\psi. \end{aligned}$$

Paso 2 (FN2).
Exteriorización de $\wedge$ u $\vee$, esto es, la propia obtención de la forma normal.

$$\phi \vee (\psi \wedge \chi) \equiv (\phi \vee \psi) \wedge (\phi \vee \chi) \text{ —si buscamos FNC—;}$$

[9] Normalform https://www.mathematik.uni-marburg.de/~thormae/lectures/ti1/code/normalform/index.html, de Thorsten Thormählen (https://www.uni-marburg.de/en/fb12/research-groups/grafikmultimedia/thormae).

$$\phi \wedge (\psi \vee \chi) \equiv (\phi \wedge \psi) \vee (\phi \wedge \chi) \text{ —si buscamos FND—.}$$

Paso 3 (FN3).
Simplificación y ordenación de los resultados (optativamente).

0. suprimir las redundancias mediante las reglas de indempotencia: $\phi \wedge \phi \equiv \phi$ y $\phi \vee \phi \equiv \phi$;
1. ordenar alfabéticamente, mediante conmutativas:
   0. si se tiene FNC, sus disyunciones miembro:
      $\phi \vee \psi \equiv \psi \vee \phi$;
   1. si se tiene FND, sus conjunciones miembro:
      $\phi \wedge \psi \equiv \psi \wedge \phi$.

Teorema 3.1 (Obtención de la forma normal de una fórmula)
Mediante el procedimiento anterior se obtienen las formas normales disyuntiva y conjuntiva de una fórmula dada.

Ejemplo 148

El ejemplo 150 (pág. 264 de esta edición) ilustrará este procedimiento.

§ 3.1.4 Estrategia de formas normales sobre la validez de una fórmula

Mediante la utilización de las dos siguientes reglas es posible decidir si una fórmula es insatisfactible, contingente o válida.

Teorema 3.2 (Regla FNC)
Una fórmula en FNC es una fórmula válida si, y sólo si, en cada cláusula aparece una variable y su negación.

Teorema 3.3 (Regla FND)
Una fórmula en FND es una fórmula insatisfactible si, y sólo si, en cada cubo aparece una variable y su negación.

Ejemplo 149

Demostremos que:

0. $(p \wedge \neg p \wedge q) \vee (p \wedge q \wedge \neg q)$ es una fórmula insatisfactible;
1. $(p \vee \neg p \vee q) \wedge (p \vee q \vee \neg q)$ es una fórmula válida;
2. $p \vee q$ es una fórmula contingente.

Resolución.— En efecto,

0. $(p \wedge \neg p \wedge q) \vee (p \wedge q \wedge \neg q)$ está en FND, y es una fórmula insatisfactible porque en cada cubo aparece una variable y su negación;

1. $(p \vee \neg p \vee q) \wedge (p \vee q \vee \neg q)$ está en FNC, y es una fórmula válida porque en cada cláusula aparece una variable y su negación;

2. $p \vee q$ no es una fórmula insatisfactible porque expresada en FND, sus cubos son p y q, por lo que no es cierto que en cada cubo aparezca una variable y su negación; por otro lado, tampoco es una fórmula válida, pues expresada en FNC, tiene una única cláusula, a saber, $p \vee q$, por lo que no es cierto que en cada cláusula aparezca una variable y su negación; por lo tanto, $p \vee q$ es una contingencia. ■

Observación 3.1.4.— Fijémonos en cómo en el último ejemplo hemos usado las versiones contrapositivas (o, sinónimamente, coinversas) de las reglas FNC y FND, esto es:

Regla FNC contrapositiva.— Una fórmula en FNC no es una fórmula válida si, y sólo si, no es cierto que en cada cláusula aparece una variable y su negación.

Regla FND contrapositiva.— Una fórmula en FND no es una fórmula insatisfactible si, y sólo si, no es cierto que en cada cubo aparece una variable y su negación.

Veamos ahora otro ejemplo donde además aplicamos el procedimiento de obtención de las formas normales estudiado en el teorema 3.1 (pág. 263 de esta edición).

Ejemplo 150

«Es absolutamente falso que si votas, entonces si eres mayor de edad, votas».

¿Es esta afirmación una contradicción?

[Cubit 29].

Resolución.— Siendo:

$p \leftrightharpoons$ tú votas,

$q \leftrightharpoons$ tú eres mayor de edad,

la fórmula en lógica de juntores que corresponde a esta afirmación es id$\neg(p \to (q \to p))$, esto es, $\neg(p \to (q \to p))$.

Así, la cuestión es si $\neg(p \to (q \to p))$ es una fórmula insatisfactible, esto es si $p \to (q \to p)$ es una fórmula válida —punto de vista semántico, de la teoría de modelos—, o equivalentemente —debido a que la lógica de juntores es correcta y completa[10]—, si $p \to (q \to p)$ es un teorema lógico —punto de vista sintáctico, de la teoría de la demostración—.

Vía 0.

Abordemos primero su *análisis mediante formas normales disyuntivas* (FND).

Hallemos su forma normal disyuntiva (FND)[11] y decidamos —$[TI]$ denota el teorema de intercambio[12] y $FN0$, $FN1$, $FN2$ y $FN3$ son las correspondientes guías para obtener una forma normal[13]—.

0.	$\neg(p \to (q \to p)) \equiv$	
1.	$\equiv \neg(\neg p \vee (\neg q \vee p))$	$[TI][FN0]$ a $\{0\}$
2.	$\equiv \neg\neg p \wedge \neg(\neg q \vee p)$	$[TI][FN1]$ a $\{1\}$
3.	$\equiv p \wedge \neg\neg q \wedge \neg p$	$[TI][FN1]$ a $\{2\}$
4.	$\equiv p \wedge q \wedge \neg p$	$[TI][FN1]$ a $\{3\}$
5.	$\equiv p \wedge \neg p \wedge q$	$[TI][FN3]$ a $\{4\}$

La FND sólo tiene un cubo, y efectivamente, en él aparece una variable, p, y su negación, $\neg p$, luego, por la Regla FND —teorema 3.3 (pág. 263 de esta edición)—, la fórmula $\neg(p \to (q \to p))$ es insatisfactible. □

Vía 1.

Hagamos ahora su *análisis mediante formas normales conjuntivas* (FNC).

Observemos que la FND anterior puede ser vista como una forma normal conjuntiva (FNC)[14].

Sin embargo, la Regla FNC —teorema 3.2 (pág. 263 de esta edición)— nos informa de que la fórmula no es válida, dejándonos con la duda de si es contingente o insatisfactible. De hecho, lo que debemos asegurar es que la fórmula $\neg(p \to (q \to p))$ es insatisfactible, o equivalentemente, que la fórmula $p \to (q \to p)$ es válida.

[10] *Cfr. infra* teorema 6.9 (pág. 446 de esta edición).
[11] *Cfr. supra* definición 3.1 (pág. 258 de esta edición).
[12] *Cfr. supra* teorema 1.17 (pág. 158 de esta edición).
[13] *Cfr. supra* teorema 3.1 (pág. 263 de esta edición).
[14] *Cfr. supra* teorema 3.0 (pág. 258 de esta edición)

Como hemos obtenido que $\neg(p \to (q \to p)) \equiv p \wedge \neg p \wedge q$, tenemos que $p \to (q \to p) \equiv \neg(p \wedge \neg p \wedge q)$.

Expresemos esta última en FNC:

0.	$\neg(p \wedge \neg p \wedge q) \equiv$	
1.	$\equiv \neg p \vee \neg\neg p \vee \neg q$	$[TI][FN1]$ a $\{0\}$
2.	$\equiv \neg p \vee p \vee \neg q$	$[TI][FN1]$ a $\{1\}$

La FNC sólo tiene una cláusula, y efectivamente, en ella aparece una variable, p, y su negación, $\neg p$, luego, por la Regla FNC —teorema 3.2 (pág. 263 de esta edición)—, $p \to (q \to p)$ —o la fórmula lógicamente equivalente, $\neg(p \wedge \neg p \wedge q)$— es una fórmula válida, por lo que su negación es una fórmula insatisfactible.

Solución.— Sí, la afirmación es una contradicción. ■

Ejemplo 151

Recordemos el ejemplo 96 (pág. 134 de esta edición). Allí demostramos con una tabla de verdad que es válida la argumentación $\mathcal{B}$ publicada por el medio de comunicación, a saber: «Si hay menos automóviles en las carreteras, la contaminación será aceptable. O bien tenemos menos automóviles en las carreteras, o bien se tendría que cobrar por el uso de las carreteras, o bien ambas cosas. Si se cobra por usar las carreteras, la temperatura aumentará en verano hasta un nivel insoportable. Este verano la temperatura está resultando ser bastante agradable. La conclusión es ineludible: la contaminación es aceptable». Pues bien, se trata aquí de que demostremos su validez por formas normales. (Es aceptable utilizar un artefacto en línea).

Resolución.— Utilicemos para ello, el artefacto en línea PBL[15]. La entrada correspondiente a la expresión en lógica de juntores de $\mathcal{B}$,

```
((C => P) & (C | S) & (S => H) & ~H) => P
```

nos la habría devuelto reescrita en forma normal conjuntiva

```
(C | ~C | S | H | P) &
(C | ~C | ~H | H | P) &
(C | ~S | S | H | P) &
(C | ~S | ~H | H | P) &
(~P | ~C | S | H | P) &
(~P | ~C | ~H | H | P) &
```

[15] PBL (http://formal.cs.utah.edu:8080/pbl/PBL.php) de Tyler Sorensen (https://github.com/tyler-utah).

```
(~P | ~S | S | H | P) &
(~P | ~S | ~H | H | P)
```

en la que observamos que en toda cláusula hay un literal y su opuesto —una variable proposicional y su negación—, por lo que por un teorema conocido, la fórmula es una fórmula válida y, por tanto, el argumento B es válido. ■

Observación 3.1.5.— Pudiésemos utilizar el artefacto en línea SageMath[16] y el siguiente programita en lenguaje Sage que aprovecha la biblioteca SymPy[17],

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
# utilizando SymPy
from sympy import symbols
from sympy.logic.boolalg import And, Or, Not, Implies, Equivalent, to_cnf
# definiendo las variables proposicionales
C, P, S, H = symbols('C P S H')
# definiendo la fórmula
formula = Implies(
        And(
                Implies(C, P),
                Or(C, S),
                Implies(S, H),
                Not(H)
        ),
        P
)
# convirtiendo la fórmula a su forma normal conjuntiva (FNC)
fnc_formula = to_cnf(formula)
# mostrando la fnc
print(f"FNC: {fnc_formula}")
```

cuya ejecución proporciona:

```
FNC: (C | H | P | S | ~C) & (C | H | P | S | ~S) & (C | H | P | ~C | ~H) & (C | H | P |
~H | ~S) & (H | P | S | ~C | ~P) & (H | P | S | ~P | ~S) & (H | P | ~C | ~H | ~P) & (H
| P | ~H | ~P | ~S)
```

O también éste más corto:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
# referencia: https://doc.sagemath.org/html/en/reference/logic/index.html
#
f = propcalc.formula("((C -> P) & (P | S) & (S -> H) & ~H) -> P") # introducimos la fórmula
f.convert_cnf_recur() # hallamos la forma normal conjuntiva de la fórmula
f # la mostramos
```

[16] *Cfr. supra* § 11 (pág. cii de esta edición).
[17] *Vid.* https://doc.sagemath.org/html/en/reference/spkg/sympy.html.

cuya ejecución proporciona:

```
(C | ~C | S | H | P) & (~P | ~C | S | H | P) & (C | ~S | S | H | P) & ( ~P | ~S | S | H
| P) & (C | ~C | ~H | H | P) & ( ~P | ~C | ~H | H | P) & (C | ~S | ~H | H | P) & ( ~P |
~S | ~H | H | P)
```

O éste:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
# referencia: https://doc.sagemath.org/html/en/reference/logic/index.html
#
f = propcalc.formula("((C -> P) & (P | S) & (S -> H) & ~H) -> P") # introducimos la fórmula
f.convert_cnf_table() # hallamos la forma normal conjuntiva de la fórmula
f # la mostramos
```

cuya ejecución proporciona:

```
(C | ~C)
```

simplificada, en la que es mucho más sencillo observar que se trata de una fórmula válida.

Si bien pudiese ser interesante que lo programásemos desde cero (*cfr.* actividad 3.2 [pág. 269 de esta edición]).

Observación 3.1.6.— Otro artefacto en línea es LogEx[18]. Este artefacto transforma una fórmula a forma normal disyuntiva y a forma normal conjuntiva, además demuestra equivalencias lógicas por encadenamiento de equivalencias, y todo esto, mostrando ayuda para que vayamos construyendo, si queremos, la demostración e incluso puede mostrarnos ésta completa, con todos los pasos.

Observación 3.1.7.— La colección de todas las fórmulas insatisfactibles, la de todas las fórmulas contingentes y la de todas las fórmulas válidas son *conjuntos decidibles*. Esto es así porque existe un algoritmo de decisión para conocer si una fórmula dada es insatisfactible, contingente o válida. De hecho, esto ya lo sabíamos, pues sí que teníamos un algoritmo, la estrategia de las tablas de verdad. Aquí lo hemos corroborado mediante otro algoritmo, la estrategia de las formas normales.

Observación 3.1.8.— Visto lo visto en el ejemplo 150 (pág. 264 de esta edición), «si votas, entonces si eres menor de edad, votas» también es una afirmación válida, ¿o no?

Actividad 3.0

Utilicemos formas normales para determinar si $(p \vee q) \to (p \wedge q)$ es una fórmula insatisfactible, contingente o válida.

[Cubit 31].

---

[18] LogEx (https://ideas.science.uu.nl/logex/) del equipo Ideas (https://ideas.science.uu.nl/), principalmente de personal de la *Universiteit Utrecht* y de la *Open Universiteit*, de Países Bajos.

Actividad 3.1

Utilicemos formas normales para determinar si $(p \wedge q) \rightarrow (p \vee q)$ es una contradicción, una indeterminación o una tautología.

[Cubit 32].

Actividad 3.2

Creemos un programa para hallar las formas normales conjuntiva y disyuntiva de una fórmula dada. Si bien el lenguaje de programación es a nuestra entera elección, el diseño debiese seguir el algoritmo para la obtención de formas normales*—.

* *Vid. supra* § 3.1.3 (pág. 262 de esta edición).

§ 3.1.5 Otras formas de representación, algunas mínimas

Dada una base de juntores y dos fórmulas ϕ y ψ con juntores únicamente de dicha base, decimos que ψ es una *representación mínima* de ϕ precisamente si son lógicamente equivalentes y en la expresión de ψ participan el menor número posible de constantes, variables y de juntores de dicha base.

Hemos visto:

0. forma normal disyuntiva (FND);

1. forma normal conjuntiva (FNC).

Tenemos además:

2. forma normal algebraica (FNA) (base de juntores $\{\wedge, \veebar\}$) (disyunción exlusiva de cubos)

3. forma normal negativa (FNN) (base de juntores $\{\neg, \vee, \wedge\}$) (pero el negador sólo a variables; FNC y FND son FNN)

Se utilizan diferentes bases de juntores y formas de representación. Por ejemplo, en la presentación estándar de Wolfram|Alpha aparecen FND, FNC, FNA y además las formas:

4. NOR (base de juntores $\{\neg, \overline{\vee}\}$)

5. NAND (base de juntores $\{\neg, \overline{\wedge}\}$)

6. AND (base de juntores $\{\neg, \wedge\}$)

7. OR (base de juntores $\{\neg, \vee\}$)

8. BOOLE (base de juntores no minimal $\{\neg, \vee, \wedge, \veebar, \rightarrow, \leftrightarrow\}$)

9. BIT2 (base de juntores no minimal $\{\neg, \vee, \wedge, \veebar\}$)

10. IMPLIES (base de juntores $\{\neg, \rightarrow\}$)

11. ESOP (suma exclusiva de productos) (base de juntores $\{\neg, \wedge, \veebar\}$)

12. ITE (If-Then-Else) (base de juntores $\{\neg, \vee, \wedge\}$, con la estructura $(\phi \wedge \psi) \vee (\neg\phi \wedge \chi)$, si bien como ya comentamos en la observación 1.3.53 (pág. 112 de esta edición), parece mucho más clara la expresión lógicamente equivalente $(\phi \rightarrow \psi) \wedge (\neg\phi \rightarrow \chi)$.

Ejemplo 152

Sea $(p \wedge q) \vee (\neg p \wedge r)$ —o su equivalente lógica $(p \rightarrow q) \wedge (\neg p \rightarrow r)$—. Utilizando el artefacto en línea Wolfram|Alpha hallemos para ella todas las formas anteriores.

Resolución.— Son las siguientes:

0. FND: $(p \wedge q) \vee (\neg p \wedge r)$;
1. FNC: $(\neg p \vee q) \wedge (p \vee r)$;
2. FNA: $r \veebar (p \wedge q) \veebar (p \wedge r)$;
3. FNN: $(p \wedge q) \vee (\neg p \wedge r)$;
4. NOR: $(\neg p \veebar q) \veebar (p \veebar r)$;
5. NAND: $(p \barwedge q) \barwedge (\neg p \barwedge r)$;
6. AND: $\neg(p \wedge \neg q) \wedge \neg(\neg p \wedge \neg r)$;
7. OR: $\neg(\neg p \vee \neg q) \vee \neg(p \vee \neg r)$;
8. BOOLE: $(p \wedge q) \vee (\neg p \wedge r)$;
9. BIT2: $r \veebar (p \wedge (q \veebar r))$;
10. IMPLIES: $(p \rightarrow \neg q) \rightarrow \neg(r \rightarrow p)$;
11. ESOP: $(q \wedge r) \veebar (\neg p \wedge \neg q \wedge r) \veebar (p \wedge q \wedge \neg r)$;
12. ITE: $(p \wedge q) \vee (\neg p \wedge r)$. ■

Observación 3.1.9.— Además de con el artefacto en línea Wolfram|Alpha, es posible obtener expresiones en FNC y FND con otros artefactos lógicos al uso; por ejemplo:

- con Logic Calculator[19], ejecutando la entrada `(((((~ p & q) & r) & (~ p v q)) & (q v ~ r)) & (q v ~ s)) -> (p & ~ q)`;
- con SageMath[20], ejecutando el código (el lenguaje es Sage)

```
fórmula = propcalc.formula("(~p&q&r&(~p|q)&(q|~r)&(q|~s))->(p&~q)")
fórmula.convert\_cnf\_table()
fórmula
```

[19] Logic Calculator —de Christian Gottschall (https://www.erpelstolz.at/christian/homepage-uk.html), en Gateway to Logic (https://www.erpelstolz.at/gateway/)—, en su versión del lado del servidor, debemos elegir en el desplegable «Task to be performed» [Tarea para ser realizada], «Conjunctive normal form (CNF)» [Forma normal conjuntiva (FNC)] —si bien probablemente sea una buena idea volver a leer lo escrito sobre Logic Calculator en la observación 1.8.1 (pág. 134 de esta edición) para recordar la sintaxis ya aprendida en su uso como generador de tablas de verdad—.

[20] *Cfr. supra* § 11 (pág. cii de esta edición).

§ 3.1.6 Tablas de decisión

Una *tabla de decisión*[21] representa la lógica de una cuestión en función de unas *reglas de decisión* que determinan qué *tratamientos* —definidos por un conjunto de *acciones*— ejecutar a partir de unas *situaciones* dadas —definidas por un conjunto de *condiciones*—.

Una *tabla de decisión bivalente* es aquélla en la que cada condición se evalúa con dos valores ((S)í, (N)o; (V)erdadero, (F)also; 0, 1; etc.); una *tabla de decisión multivalente* es aquélla en la que cada condición se evalúa con más de dos valores; una *tabla de decisión mixta* es aquélla en la que existen condiciones que se evalúan bivalentemente y condiciones que se evalúan multivalentemente. La evaluación de una condición puede incluir indiferencia.

Una tabla de decisión pudiese presentar *redundancia* (si existiesen una o más situaciones repetidas) o *inconsistencia* (si presentase redundancia y existiesen situaciones repetidas con distinto tratamiento).

En ocasiones, puede simplificarse una tabla de decisión; estrategias útiles para ello en las tablas bivalentes son: la *regla del paraguas* (cuando se detecten reglas con igual tratamiento que varían sólo en el valor de una condición) y los *mapas de* KARNAUGH.

A modo de ejemplo, una tabla de decisión bivalente es la siguiente.

		Reglas de decisión							
		Situaciones							
Condiciones	Condición 0 (c_0)	0	0	0	0	1	1	1	1
	Condición 1 (c_1)	0	0	1	1	0	0	1	1
	Condición 2 (c_2)	0	1	0	1	0	1	0	1
		Tratamientos							
Acciones	Acción 0 (a_0)		✓						✓
	Acción 1 (a_1)	✓	✓	✓					
	Acción 2 (a_2)	✓			✓			✓	
	Acción 3 (a_3)	✓			✓	✓	✓	✓	
	Acción 4 (a_4)	✓	✓	✓		✓		✓	

Pudiésemos usar la notación CPL del operador condicional[22] para expresar la forma lógica correspondiente al anidamiento de alternativas proporcionado por este ejemplo de tabla de decisión:

$$c_0 \land c_1 \land c_2 \to a_0, (c_0 \land c_1 \land \neg c_2 \to a_2 \land a_3 \land a_4, (c_0 \land \neg c_1 \land c_2 \to a_3, (c_0 \land \neg c_1 \land \neg c_2 \to a_3 \land a_4, (\neg c_0 \land c_1 \land c_2 \to a_2 \land a_2 \land a_3, (\neg c_0 \land c_1 \land \neg c_2 \to a_1 \land a_4, (c_0 \land \neg c_1 \land c_2 \to a_0 \land a_1 \land a_4, a_1 \land a_2 \land a_3 \land a_4))))))).$$

[21] *Vid. v. gr.* https://en.wikipedia.org/wiki/Decision_table.
[22] *Cfr. supra* pág. 112 de esta edición.

§ 3.2 Dualidad

Definición 3.7.— Dada una fórmula ϕ generada por la base de juntores $\{\neg, \vee, \wedge\}$, llamamos *fórmula dual* de ϕ y notamos por ϕ', a la que resulta de sustituir en ϕ todas las apariciones de $\vee$ por $\wedge$ y las de $\wedge$ por $\vee$, sin modificar las apariciones de $\neg$.

Tenemos los siguientes principios (o metateoremas) de dualidad.

Teorema 3.4 (DU0)
La negación de la dual de una fórmula válida también es una fórmula válida, esto es,

$$\text{si } \phi \dashv\models \top, \text{ entonces } \neg\phi' \dashv\models \top,$$

en otras palabras,

$$\text{si } \models \phi, \text{ entonces } \models \neg\phi',$$

es decir, si ϕ es una fórmula válida, entonces $\neg\phi'$ es una fórmula válida.

Teorema 3.5 (DU1)
Si dos fórmulas son lógicamente equivalentes, también lo son sus duales, esto es,

$$\text{si } \phi \dashv\models \psi, \text{ entonces } \phi' \dashv\models \psi',$$

en otras palabras,

$$\text{si } \models \phi \leftrightarrow \psi, \text{ entonces } \models \phi' \leftrightarrow \psi',$$

es decir, si $\phi \leftrightarrow \psi$ es una fórmula válida, entonces $\phi' \leftrightarrow \psi'$ es una fórmula válida.

Teorema 3.6 (DU2)
Si una fórmula implica lógicamente una segunda, la dual de ésta implica lógicamente la dual de la primera, esto es,

$$\text{si } \phi \models \psi, \text{ entonces } \psi' \models \phi',$$

en otras palabras,

$$\text{si } \models \phi \to \psi, \text{ entonces } \models \psi' \to \phi',$$

es decir, si $\phi \to \psi$ es una fórmula válida, entonces $\psi' \to \phi'$ es una fórmula válida.

Observación 3.2.0.— Por ser la lógica de juntores correcta y completa[23], existe la correspondiente *versión sintáctica de los principios de dualidad*:

[23] *Cfr. infra* teorema 6.9 (pág. 446 de esta edición).

DU0. La negación de la dual de un teorema lógico también es un teorema lógico, esto es,

$$\text{si } \vdash \phi, \text{ entonces } \vdash \neg\phi'.$$

DU1. Si dos fórmulas se deducen (formalmente) mutuamente, también se deducen (formalmente) mutuamente sus duales, es decir,

$$\text{si } \vdash \phi \leftrightarrow \psi, \text{ entonces } \vdash \phi' \leftrightarrow \psi'.$$

DU2. Si de una fórmula se deduce formalmente una segunda, de la dual de ésta se deduce formalmente la dual de la primera, o sea,

$$\text{si } \vdash \phi \to \psi, \text{ entonces } \vdash \psi' \to \phi'.$$

Ejemplo 153

Demostremos:

0. si $\phi \vee \neg\phi$, entonces $\neg(\phi \wedge \neg\phi)$, esto es, el principio de la no contradicción (PNC) se deduce por dualidad del principio del tercio excluso (PTE);
1. si $(\phi \wedge \psi) \wedge \chi \mathrel{=}\!\mathrel{\mid}\!\mathrel{\models} \phi \wedge (\psi \wedge \chi)$, entonces $(\phi \vee \psi) \vee \chi \mathrel{=}\!\mathrel{\mid}\!\mathrel{\models} \phi \vee (\psi \vee \chi)$, esto es, la ley asociativa de la disyunción (AD) se deduce por dualidad de la asociativa de la conjunción (AC);
2. si $\phi \wedge \psi \to \phi$, entonces $\phi \to \phi \vee \psi$, esto es, la introducción de la disyunción (ID) se deduce por dualidad de la eliminación de la conjunción (EC);
3. si $\phi \vee \psi \mathrel{=}\!\mathrel{\mid}\!\mathrel{\models} \neg(\neg\phi \wedge \neg\psi)$, entonces $\phi \wedge \psi \mathrel{=}\!\mathrel{\mid}\!\mathrel{\models} \neg(\neg\phi \vee \neg\psi)$, esto es, De Morgan 1 ($DM_1$) se deduce por dualidad de De Morgan 0 (DM_0).

[Cubit 30].

Resolución.— Las cuatro son inmediatas: 0., por DU0; 1. y 3., por DU1, y 2., por DU2. ■

Lengua - lenguaje

Si {actor, actriz}, entonces {narrador, narratriz}.

§ 3.2.0 Estrategia de dualidad sobre la validez de una fórmula

Como muestra de la estrategia que aportan los metateoremas de dualidad estudiados en el teorema 3.2 (pág. 272 de esta edición), tenemos:

0. las dualidades existentes entre las correspondientes leyes:
   0. conmutativa (CoC = CoD′),

1. asociativa ($AC = AD'$),

2. de idempotencia ($IdC = IdD'$),

3. de absorción ($AbsC = AbsD'$) y

4. distributiva ($DisC = DisD'$),

para los juntores conjuntor y disyuntor, estudiadas en § 233 (pág. 208 de esta edición); de hecho, suelen demostrarse dichas leyes para el conjuntor y aplicando después DU2 se tienen para el disyuntor;

1. las dualidades:

   0. entre la definición del disyuntor a partir del negador y el conjuntor y la del conjuntor a partir del negador y el disyuntor ($DC_0 = DD'_0$), y

   1. entre las correspondientes leyes de De Morgan ($DM_1 = DM'_0$),

todas ellas estudiadas en § 233 (pág. 217 de esta edición).

§ 3.3 Tablas analíticas/semánticas

Este subcapítulo versa sobre un método que utilizaremos, fundamentalmente, para decidir

0. si una fórmula ϕ es válida, esto es, si $\vDash \phi$, o

1. si una fórmula ψ es consecuencia lógica de un conjunto Φ de fórmulas, esto es, si $\Phi \vDash \psi$.

Aunque estudiamos este método en la semántica, por ser L_0 —la lógica de juntores— correcta (consistente) y completa, igualmente pudiésemos haberlo hecho en la sintaxis con el cuidado de no hablar de verdad ni falsedad, siendo entonces los objetivos decidir

0. si una fórmula ϕ es un teorema lógico, esto es, si $\vdash \phi$, o

1. si una fórmula ψ es formalmente deducible (derivable) de Φ, esto es, si $\Phi \vdash \psi$.

En cualquier caso, el problema sintáctico es reducible al semántico.

Adaptamos las tablas analíticas de Smullyan [67], variante de las tablas semánticas de Beth [90] y las tablas de Hintikka [91].

El proceso de construcción de la tabla puede representarse mediante un árbol lógico. Las fórmulas implicadas y subfórmulas suyas, se organizarán como etiquetas de los nodos de un árbol enraizado diádico ordenado, árbol que se irá extendiendo, todo ello de acuerdo a lo que aprenderemos a continuación. En la lógica de juntores este árbol siempre es finito; en la de cuantores, a veces será infinito.

Crucial para su construcción será saber si una expresión tiene una estructura «profunda» conjuntiva o disyuntiva. En vez de analizar todos los juntores, basta hacerlo para una base cualquiera; lo haremos para la base $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$, por lo que se trata de conocer dicha estructura para cada uno de estos juntores y para sus negaciones, en otras palabras, sus formas normales disyuntivas o conjuntivas, según sea el caso.

Examinamos el método diferenciando *reglas semánticas* y *patrones de extensión*, aunque debido a la equivalencia existente entre dichas reglas y patrones, llegado el momento hablaremos simplemente de *reglas de extensión*.

§ 3.3.0 Reglas semánticas

Supongamos que conocemos si la premisa es verdadera o falsa, entonces pueden suceder dos situaciones:

0. que se bifurque la inferencia en dos expresiones alternativas, de las cuales, al menos una de las cuales ha de ser verdadera —utilizaremos el signo ╱╲ para designar esta situación—, o
1. que se infieran dos expresiones distintas, una tras otra, ambas verdaderas —utilizaremos el signo | para designar esta situación—.

Además, la designación de las situaciones por estos símbolos aporta idea gráfica sobre la expansión del árbol, como veremos más adelante (*cfr. infra* § 3.3.3 [pág. 279 de esta edición]).

Agrupamos en reglas semánticas *de verdad* (o, sinónimamente, *afirmativas*) y *de falsedad* (o, sinónimamente, *negativas*).

Reglas semánticas de verdad en L_0

Verdad de la disyunción (VD):

$$\frac{\phi \vee \psi}{\phi \quad \diagup \quad \diagdown \quad \psi}$$

Verdad de la conjunción (VC):

$$\frac{\phi \wedge \psi}{\begin{array}{c}\phi \\ | \\ \psi\end{array}}$$

Verdad de la implicación (VI)
—Principio de Filón—:

$$\frac{\phi \rightarrow \psi}{\neg\phi \quad \diagup \quad \diagdown \quad \psi}$$

Verdad de la equivalencia (VE):

$$\frac{\phi \leftrightarrow \psi}{(\phi \wedge \psi) \quad | \quad (\neg\phi \wedge \neg\psi)}$$

Reglas semánticas de falsedad en L_0

Falsedad de la negación (FN)
—Doble negación (DN)—:

$$\frac{\neg\neg\phi}{\phi}$$

Falsedad de la disyunción (FD)
—Ley de De Morgan DM_0—:

$$\frac{\neg(\phi \vee \psi)}{\neg\phi \;\; | \;\; \neg\psi}$$

Falsedad de la conjunción (FC)
—Ley de De Morgan DM_1—:

$$\frac{\neg(\phi \wedge \psi)}{\neg\phi \quad | \quad \neg\psi}$$

Falsedad de la implicación (FI)
—Principio de Crisipo—:

$$\frac{\neg(\phi \rightarrow \psi)}{\phi \;\; | \;\; \neg\psi}$$

Falsedad de la equivalencia (FE):

$$\frac{\neg(\phi \leftrightarrow \psi)}{(\phi \wedge \neg\psi) \quad | \quad (\neg\phi \wedge \psi)}$$

§ 3.3.1 Patrones de extensión

Distinguimos dos tipos de fórmulas. Cada *fórmula conjuntiva* (o, sinónimamente, *fórmula-α* y cada *fórmula disyuntiva* (o, sinónimamente, *fórmula-β*) tiene asociadas dos componentes, de tal forma que $\alpha \equiv \alpha_0 \wedge \alpha_1$ y $\beta \equiv \beta_0 \vee \beta_1$. Esto origina la distinción entre *patrón de extensión conjuntivo* (o, sinónimamente, *patrón de extensión de tipo α*) y *patrón de extensión disyuntivo* (o, sinónimamente, *patrón de extensión de tipo β*).

Dadas la base de juntores $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$, son los siguientes.

Patrones de extensión de tipo α en L_0

Para las fórmulas-α, aquéllas en las que el signo principal es $\wedge$.

	α	α_0	α_1
Falsedad de la negación (FN):	$\neg\neg\phi$	ϕ	ϕ
Verdad de la conjunción (VC):	$\phi \wedge \psi$	ϕ	ψ
Falsedad de la disyunción (FD):	$\neg(\phi \vee \psi)$	$\neg\phi$	$\neg\psi$
Falsedad de la implicación (FI):	$\neg(\phi \rightarrow \psi)$	ϕ	$\neg\psi$

Patrones de extensión de tipo β en L_0

Para las fórmulas-β, aquéllas en las que el signo principal es $\vee$.

	β	β_0	β_1
Falsedad de la conjunción (FC):	$\neg(\phi \wedge \psi)$	$\neg\phi$	$\neg\psi$
Verdad de la disyunción (VD):	$\phi \vee \psi$	ϕ	ψ
Verdad de la implicación (VI):	$\phi \rightarrow \psi$	$\neg\phi$	ψ
Verdad de la equivalencia (VE):	$\phi \leftrightarrow \psi$	$\phi \wedge \psi$	$\neg\phi \wedge \neg\psi$
Falsedad de la equivalencia (FE):	$\neg(\phi \leftrightarrow \psi)$	$\phi \wedge \neg\psi$	$\neg\phi \wedge \psi$

Como intuimos y apreciamos, hay una correspondencia biyectiva entre las reglas semánticas y los patrones de extensión.

Observación 3.3.0.— Encontramos otros nombres y abreviaturas en la literatura. Un ejemplo, en el orden mostrado, para los patrones conjuntivos: *negación de la conjunción* (NC), *disyunción* (D), *implicación* (I), *equivalencia* (E) y *negación de la equivalencia* (NE); para los disyuntivos: *doble negación* (DN), *conjunción* (C), *negación de la disyunción* (ND) y *negación de la implicación* (NI).

Observación 3.3.1.— Hemos considerado la base de juntores $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$. Claramente, para el resto de juntores o sus negaciones tenemos también reglas y patrones, por ejemplo:

	α	α_0	α_1
Falsedad de la contravalencia (FCv):	$\neg(\phi \veebar \psi)$	$\neg\phi \vee \psi$	$\phi \vee \neg\psi$
Falsedad de la replicación (FR):	$\neg(\phi \leftarrow \psi)$	$\neg\phi$	ψ
Verdad de la desimplicación (FR):	$\phi \nrightarrow \psi$	ϕ	$\neg\psi$
Verdad de la desreplicación (FR):	$\phi \nleftarrow \psi$	$\neg\phi$	ψ
Falsedad de la incompatibilidad (FIc):	$\neg(\phi \mid \psi)$	ϕ	ψ
Verdad de la negación conjunta (VNc):	$\phi \downarrow \psi$	$\neg\phi$	$\neg\psi$

	β	β_0	β_1
Verdad de la contravalencia (VCv):	$\phi \veebar \psi$	$\phi \wedge \neg\psi$	$\neg\phi \wedge \psi$
Falsedad de la contravalencia (FCv):	$\neg(\phi \veebar \psi)$	$\phi \wedge \psi$	$\neg\phi \wedge \neg\psi$
Verdad de la replicación (VR):	$\phi \leftarrow \psi$	ϕ	$\neg\psi$
Falsedad de la desimplicación (FR):	$\neg(\phi \nrightarrow \psi)$	$\neg\phi$	ψ
Falsedad de la desreplicación (FR):	$\neg(\phi \nleftarrow \psi)$	ϕ	$\neg\psi$
Verdad de la incompatibilidad (VIc):	$\phi \mid \psi$	$\neg\phi$	$\neg\psi$
Falsedad de la negación conjunta (FNc):	$\neg(\phi \downarrow \psi)$	ϕ	ψ

Observación 3.3.2.— La verdad y falsedad de la contravalencia y de la equivalencia pueden expresarse como patrones α:

	α	α_0	α_1
Verdad de la contravalencia (VCv$_\alpha$):	$\phi \veebar \psi$	$\neg\phi \vee \neg\psi$	$\phi \vee \psi$
Falsedad de la contravalencia (FCv$_\alpha$):	$\neg(\phi \veebar \psi)$	$\neg\phi \vee \psi$	$\phi \vee \neg\psi$
Verdad de la equivalencia (VE$_\alpha$):	$\phi \leftrightarrow \psi$	$\neg\phi \vee \psi$	$\phi \vee \neg\psi$
Falsedad de la equivalencia (FCv$_\alpha$):	$\neg(\phi \leftrightarrow \psi)$	$\neg\phi \vee \neg\psi$	$\phi \vee \psi$

pero su utilización llevaría a una complicación innecesaria de la estructura de la tabla.

Observación 3.3.3.— Si bien hemos expresado las componentes resultantes α_0, α_1, β_0 y β_1 en la base de juntores $\{\neg, \wedge, \vee\}$, somos libres de utilizar otros juntores, por ejemplo,

	α	α_0	α_1
Verdad de la equivalencia (VE$_0$):	$\phi \leftrightarrow \psi$	$\phi \rightarrow \psi$	$\psi \rightarrow \phi$

	β	β_0	β_1
Falsedad de la equivalencia (FE$_0$):	$\neg(\phi \leftrightarrow \psi)$	$\neg(\phi \rightarrow \psi)$	$\neg(\psi \rightarrow \phi)$

aunque al no seguir la naturaleza de la construcción de la tabla supondría una complicación innecesaria de la estructura de la misma.

§ 3.3.2 Satisfactibilidad de ramas y árboles

Definición 3.8.— Una *rama satisfactible* es aquélla en la que el conjunto de fórmulas que etiquetan sus nodos es un conjunto satisfactible de fórmulas[24]. Una *rama insatisfactible* es aquélla en la que dicho conjunto es un conjunto insatisfactible de fórmulas —pensemos, por ejemplo, en un conjunto al que pertenezca una fórmula insatisfactible o una fórmula y su negación—.

Definición 3.9.— Un *árbol satisfactible* es aquél en el que existe alguna rama satisfactible; un *árbol insatisfactible* es aquél en el que toda rama es insatisfactible.

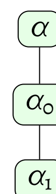
[24] *Cfr. supra* definición 1.15 (pág. 121 de esta edición).

§ 3.3.3 Reglas de extensión

Para reflejar, en cierta forma, la equivalencia entre reglas semánticas y patrones de extensión, hablamos de *reglas de extensión*. Éstas, la regla-α y la regla-β, nos permiten extender un árbol introduciendo subfórmulas de las fórmulas que etiquetan ciertos nodos de dicho árbol.

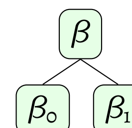
Definición 3.10.— Sea ϕ una fórmula que etiqueta un nodo hoja; si la rama ρ de la cual ϕ es nodo hoja, es satisfactible y el nodo ϕ no está etiquetado con $\surd$, entonces

Regla-α:



si la fórmula-α tiene la estructura $\alpha_0 \wedge \alpha_1$, extendemos ρ con dos nuevos nodos consecutivos α_0 y α_1 (si $\alpha_0 = \alpha_1$, sólo añadimos un nodo).

Regla-β:
si la fórmula-β tiene la estructura $\beta_0 \vee \beta_1$, extendemos ρ con dos nuevos nodos, uno izquierdo y otro derecho, β_0 y β_1, esto es, obtenemos dos subramas (si $\beta_0 = \beta_1$, sólo añadimos un nodo).



La *guía para la aplicación de las reglas de extensión* se resume en las tres instrucciones siguientes:

0.ª, la regla-α sólo se aplica una vez a cada nodo que contenga una fórmula-α, tras lo que se anota, este nodo origen con el signo $\surd_n$, siendo n el identificador del nodo creado, y el nodo creado se anota con este identificador y con la abreviatura de la regla aplicada junto al identificador del nodo origen;

1.ª, la regla-β sólo se aplica una vez a cada nodo que contenga una fórmula-β, tras lo que se anotan, este nodo origen con el signo $\surd_{m,n}$, siendo m y n los identificadores de los nodos creados, y los nodos creados se anotan con estos identificadores y con la abreviatura de la regla aplicada junto al identificador del nodo origen;

2.ª, la regla-α tiene prioridad sobre la regla-β[25], y

3.ª, en cuanto detectemos que una rama es insatisfactible la etiquetamos con el signo $\times$ (aspa) y dicha rama no se extiende más.

Definición 3.11.— Una *rama completa* ρ es aquélla que satisface:

0.º, si α está en ρ, también lo están α_0 y α_1, y

1.º, si β está en ρ, entonces, o β_0 está en ρ o lo está β_1;

[25] Esta heurística evita un incremento innecesario de la complejidad del árbol, ya que aplicar primero la regla-α y después la regla-β es de menor complejidad que aplicar primero la regla-β y después la regla-α.

(informalmente, esto quiere decir que una rama es completa cuando, y sólo cuando, no sea posible expandir ningún nodo).

Definición 3.12.— Un *árbol terminado* (o, sinónimamente, acabado) es aquél en el que toda rama es insatisfactible o completa.

Teorema 3.7 (Teorema de compacidad para tablas analíticas/semánticas)
Siempre puede obtenerse un árbol terminado en un número finito de extensiones.

§ 3.3.4 Refutación para un conjunto de fórmulas

Definamos inductivamente el árbol. Sea $\Gamma = \{\phi_0, \phi_1, \ldots, \phi_n\}$ un conjunto de fórmulas.

Definición 3.13.— El *árbol inicial* para Γ es de una única rama con raíz ϕ_0 y nodos consecutivos, en orden, $\phi_1, \ldots, \phi_n$. Lo notamos T_Γ. Decimos que T es un *árbol para* Γ precisamente si existe una sucesión finita de árboles $T_0, T_1, \ldots, T_n$, tal que:

0.º, $T_0 = T_\Gamma$;

1.º, T_i se obtiene de T_{i-1} ($i \geq 1$) por aplicación de una regla de extensión, y

2.º, $T_n = T$.

Definición 3.14.— Una *refutación* para Γ es un árbol insatisfactible para Γ.

Insistamos en que al usar una estrategia de refutación para demostrar la validez de una deducción semántica nuestro propósito es refutar que existe una interpretación que satisface las premisas y no satisface la conclusión —por lo que sí que la conclusión es entonces una consecuencia lógica de las premisas—. Recordemos:

- afirmar $\{\phi_0, \phi_1\} \vDash \psi$ equivale a que $(\phi_0 \wedge \phi_1) \wedge \neg\psi$ sea una fórmula insatisfactible;
- refutar $\{\phi_0, \phi_1\} \vDash \psi$ equivale a que $(\phi_0 \wedge \phi_1) \wedge \neg\psi$ sea una fórmula satisfactible.

La esencia en lógica de juntores de esto es el principio de Crisipo[26], cuyo reflejo semántico es la afirmación:

- que $\phi \rightarrow \psi$ sea una fórmula válida equivale a que $\phi \wedge \neg\psi$ sea una fórmula insatisfactible.

Justamente de esto va lo que establece el siguiente teorema.

[26] *Cfr. supra* teorema 1.27 (pág. 166 de esta edición).

Teorema 3.8

Sean ϕ y ψ fórmulas y Φ un conjunto de fórmulas. Entonces:

0. $\vDash \phi$ [ϕ es una fórmula válida] si, y sólo si, existe una refutación para Γ, siendo $\Gamma = \{\neg\phi\}$;
1. $\Phi \vDash \psi$ [ψ es consecuencia lógica de Φ] si, y sólo si, existe una refutación para Γ, siendo $\Gamma = \Phi \cup \{\neg\psi\}$.

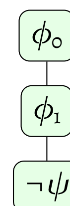
Observación 3.3.4.— Al mediar TA/S para su resolución, en el transfondo también está reducción al absurdo (Abs, RAA): si conseguimos refutar $\neg\phi$ (llegando a contradicción [$\{\neg\phi\} \vdash \bot$] en todas las ramas), entonces de RAA se sigue $\vDash \phi$.

§ 3.3.5 TA/S: el método

Resumiendo, el *método de las tablas analíticas/semánticas* (TA/S) es el siguiente:

0.º, si se trata de demostrar si ϕ es una fórmula válida, se etiqueta el nodo raíz del árbol con $\neg\phi$, siendo habitual designar el conjunto $\{\neg\phi\}$ por Γ;

1.º, si se trata de demostrar si ψ es consecuencia lógica de Φ, se disponen todas las fórmulas de Φ como etiquetas de nodos consecutivos, comenzando por la primera fórmula de Φ como nodo raíz, y a continuación, se etiqueta el siguiente nodo con $\neg\psi$ —por ejemplo, si $\Phi = \{\phi_0, \phi_1\}$, el árbol del margen—, siendo habitual designar el conjunto $\Phi \cup \{\neg\psi\}$ por Γ (esto conforma lo que llamamos un *grupo raíz* [o, sinónimamente, *raíz plural*]);



2.º, se extiende el árbol aplicando las reglas de extensión y la norma para su aplicación[27], hasta obtener un árbol terminado;

3.º, si el árbol terminado es insatisfactible, es decir, si hemos encontrado una refutación para Γ, entonces, por el teorema 3.8 (pág. 281 de esta edición), ya hemos demostrado, según sea el caso, que ϕ es una fórmula válida o que ψ es consecuencia lógica de Φ, y

4.º, si el árbol terminado es satisfactible, es decir, si no hemos encontrado una refutación para Γ, entonces, por el teorema 3.8 (pág. 281 de esta edición), ya hemos demostrado, según sea el caso, que ϕ no es una fórmula válida o que ψ no es consecuencia lógica de Φ.

Como ya hemos mencionado[28], se tiene la compacidad de TA/S; pues bien, también se satisface su consistencia y su completitud.

[27] *Cfr. supra* definición 3.10 (pág. 279 de esta edición).
[28] *Vid. supra* teorema 3.7 (pág. 280 de esta edición).

Teorema 3.9
En la lógica de juntores, TA/S es un sistema consistente (toda fórmula demostrable mediante TA/S es una fórmula válida) y completo (toda fórmula válida es demostrable mediante TA/S).

§ 3.3.6 TA/S como método de construcción de modelos

Es posible añadir algo al paso 4.º, a saber, si un árbol terminado es satisfactible, entonces encontraremos, para cada rama satisfactible,

0. uno o más modelos para $\neg\phi$, si estamos decidiendo si ϕ es una fórmula válida, o
1. uno o más modelos para $\Phi \cup \{\neg\psi\}$, si estamos decidiendo si ψ es consecuencia lógica de Φ.

Pudiese suceder que encontrásemos el mismo modelo en ramas satisfactibles distintas.

Concretamente, para cada rama satisfactible ρ, un modelo para Γ es la siguiente interpretación: para toda x, variable proposicional de cualquier fórmula de Γ, $I(x) = 1$ si x etiqueta algún nodo de ρ e $I(x) = 0$ si $\neg x$ etiqueta algún nodo de ρ.

Observación 3.3.5.— TA/S en el ámbito sintáctico.— Aunque presentamos este método en la semántica, como L_0 —la lógica de juntores— es correcta (consistente) y completa, igualmente pudiésemos haberlo presentado en la sintaxis con el cuidado de no hablar de verdad ni falsedad. En particular, en vez de rama/árbol satisfactible/insatisfactible, hablaríamos de rama/árbol abierta(o)/cerrada(o). En el ámbito sintáctico, una refutación para Γ es un árbol cerrado para Γ y el correspondiente al teorema 3.8 (pág. 281 de esta edición) reza como sigue.

Sean ϕ y ψ fórmulas y Φ un conjunto de fórmulas; entonces:

0. $\vdash \psi$ (ψ es un teorema lógico) si, y sólo si, existe una refutación para Γ, siendo $\Gamma = \{\neg\psi\}$;
1. $\Phi \vdash \psi$ (ψ se deduce/deriva formalmente de Φ) si, y sólo si, existe una refutación para Γ, siendo $\Gamma = \Phi \cup \{\neg\psi\}$.

En cualquier caso, como la lógica de juntores es correcta y completa, el problema sintáctico es reducible al semántico, esto es,

0. decidir si ϕ es un teorema lógico, esto es, si $\vdash \phi$, se reduce a decidir si ϕ es una fórmula válida, es decir, si $\vDash \phi$, y
1. decidir si ψ es formalmente deducible/derivable de Φ, esto es, si $\Phi \vdash \psi$, se reduce a decidir si ψ es consecuencia lógica de Φ, es decir, si $\Phi \vDash \psi$.

§ 3.3.7 Muestra de ejemplos de TA/S

Para todas y cada una de las afirmaciones o situaciones, que proporcionan las siguientes cuestiones, hagamos lo siguiente.

0. Hallemos el argumento equivalente a la argumentación dada. Llamemos a aquél, $\mathcal{A}$.
   - Reescribamos la argumentación. (Optativo).
   - Escribamos el argumento ($\mathcal{A}$).
   - Exploremos intuitivamente su validez. (Optativo).
1. Formalicemos dicho argumento en lógica de juntores.
   - Nombremos las variables proposicionales que representan las proposiciones simples.
   - Analicemos su estructura lógico-gramatical. (Optativo).
   - Proporcionemos su esquema argumental.
   - Hallemos su forma lógica.
2. Demostremos, utilizando TA/S, si $\mathcal{A}$ es o no es un argumento válido. Para esto, debemos:
   I. identificar el conjunto Γ de fórmulas bien formadas para el que intentamos hallar una refutación;
   II. hacer una construcción anotada del árbol semántico;
   III. demostrar de que es un árbol terminado;
   IV. demostrar la validez o no validez de $\mathcal{A}$.
3. - Si $\mathcal{A}$ resultó ser un argumento válido, finalicemos o, alternativa, mas sólo optativamente, modifiquemos las premisas o la conclusión para que el argumento modificado no sea válido, justifiquemos su no validez y continuemos.
   - Si $\mathcal{A}$ no es válido, identifiquemos los modelos que proporcionan las ramas satisfactibles.
4. Caso de que existan modelos para Γ, utilicemos alguna estrategia en lógica de juntores para demostrar que dichos modelos lo son para Γ.
5. Si existen modelos para Γ, expresemos en español las contraargumentaciones, construidas a partir de dichos modelos, que permiten refutar la argumentación dada.

Observación.— [*Metalógica de la lógica de juntores*]. Suponiendo que el argumento $\mathcal{A}$ se descompone en un conjunto $\Phi = \{\phi_0, \phi_1, \dots, \phi_n\}$ de premisas y una conclusión ψ:

- somos libres de elegir identificar formalmente $\mathcal{A}$:
  - con la deducción semántica $\Phi \vDash \psi$ (en otras palabras, ψ es conclusión lógica de Φ);
  - con $\vDash \phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \to \psi$ (esto es, $\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \to \psi$ es una fórmula válida);
  - con la deducción sintáctica $\Phi \vdash \psi$ (es decir, ψ es formalmente deducible/derivable de Φ);
  - con $\vdash \phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \to \psi$ (o sea, $\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \to \psi$ es un teorema lógico);
- con respecto a Γ, recordemos que:
  - $\Gamma = \Phi \cup \{\psi\}$ si formalizamos $\mathcal{A}$ como una deducción semántica o sintáctica;
  - $\Gamma = \{\neg(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n \to \psi)\}$ si formalizamos $\mathcal{A}$ como una fórmula válida o como un teorema lógico;
- con respecto al propio argumento, somos libres de utilizar leyes particulares para su reescritura; a modo de ejemplo, la ley de importación[29] nos permite un doble abordaje equivalente, a saber, compuesto $\mathcal{A}$ por el conjunto de premisas $\Phi = \{\phi_0, \phi_1\}$ y la conclusión ψ, bien $\phi_0 \wedge \phi_1 \to \psi$, bien $\phi_0 \to (\phi_1 \to \psi)$ (similarmente, si $\mathcal{A}$ estuviese compuesto por $\Phi = \{\phi\}$ y la conclusión $\psi_0 \to \psi_1$, pudiésemos abordarlo por $\phi \to (\psi_0 \to \psi_1)$, o por $\phi \wedge \psi_0 \to \psi_1$).

Ejemplo 154

De $\{p \vee q, p\}$, ¿se deduce q?

Resolución.—

0. *Argumento* ($\mathcal{A}$): Se tiene $p \vee q$. Se tiene p. Luego, se tiene q.

   Que reescrito destacando los juntores (recuadrados) y el deductor (subrayado), es:

   De tener p [o] q y tener p, se sigue q.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*
   - *Variables proposicionales*: p, q (vienen dadas).
   - *Esquema argumental*:

     Se tiene p o q.
     Se tiene p.

     ∴ Se sigue q.

   - *Forma lógica*.

[29] *Vid. supra* observación 2.2.17 (pág. 203 de esta edición).

Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{p \lor q, p\}$ y la conclusión ψ, a saber, q.

Por mor pedagógico, aclarando la nota anterior, digamos que cuestionarnos la validez del argumento $\mathcal{A}$ equivale a cuestionarnos:

$$\text{si } q \text{ es conclusión lógica de } \{p \lor q, p\}\text{, en otras palabras, si } \{p \lor q, p\} \vDash q; \tag{3.0}$$

$$\text{si } (p \lor q) \land p \to q \text{ es una fórmula válida, esto es, si } \vDash (p \lor q) \land p \to q; \tag{3.1}$$

$$\text{si } q \text{ es formalmente derivable de } \{p \lor q, p\}\text{, es decir, si } \{p \lor q, p\} \vdash q; \tag{3.2}$$

$$\text{si } (p \lor q) \land p \to q \text{ es un teorema lógico, o sea, si } \vdash (p \lor q) \land p \to q. \tag{3.3}$$

En este ejemplo trabajamos con la primera, $\{p \lor q, p\} \vDash q$.

Vemos, pues, que la fórmula en lógica de juntores que hemos hallado para $\mathcal{A}$ es

$$(p \lor q) \land p \to q.$$

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1\} \vDash \psi$. Refutar $\{\phi_0, \phi_1\} \vDash \psi$ es demostrar que $(\phi_0 \land \phi_1) \land \neg\psi$ es una fórmula válida.

   Como advertimos en la nota anterior, definimos Γ como el conjunto de fórmulas bien formadas

   $$\{p \lor q, p\} \cup \{\neg q\}\,,$$

   para el estudio de (3.0) o (3.2), o

   $$\{\neg(p \lor q \land p \to q)\}\,,$$

   para el estudio de (3.1) o (3.3), si bien, debido a la equivalencia de los problemas (3.0), (3.1), (3.2) y (3.3), por ser la lógica de juntores correcta y completa[30] es admisible usar estas definiciones de Γ indistintamente.

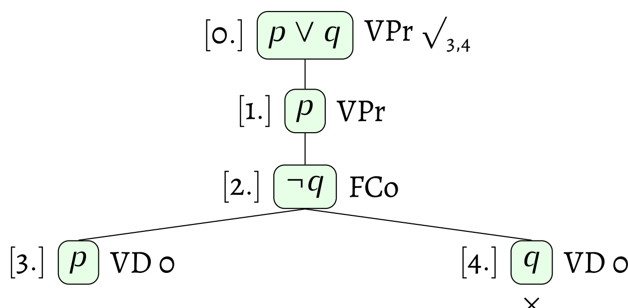
   En este ejemplo trabajamos con la primera, definimos $\Gamma = \{p \lor q, p\} \cup \{\neg q\}$.

   Estudiemos si existe una refutación para Γ —esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible—, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico.*

[30] *Vid. supra* observación 3.3.5 (pág. 282 de esta edición).

Sea el árbol:



Observación 0.—VPr ≒ Verdad de la premisa; FCo ≒ Falsedad de la conclusión; VD ≒ Verdad de la disyunción.

Observación 1.—Alternativamente, debido a la equivalencia de los problemas (3.0), (3.1), (3.2) y (3.3) pudiésemos haber comenzado el árbol por el nodo

$$\neg((p \vee q) \wedge p \to q) \qquad \text{[Falsedad de la fórmula]}$$

III. *Demostración de que es un árbol terminado.*

El tronco de este árbol es $\rho_0 = \langle p \vee q, p, \neg q \rangle$ y sus ramas son $\rho_1 = \rho_0 + \langle p \rangle = \langle p \vee q, p, \neg q, p \rangle$ y $\rho_2 = \rho_0 + \langle q \rangle = \langle p \vee q, p, \neg q, q \rangle$. La rama ρ_1 es una rama satisfactible y completa —$p \vee q$ está en ρ_1 y también está p—, mientras que ρ_2, si bien también completa, es una rama insatisfactible —dado que aparecen q y $\neg q$—. Como toda rama es insatisfactible o completa, concluimos que se trata de un árbol terminado.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existe una rama satisfactible, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), q no es consecuencia lógica de $\{p \vee q, p\}$, esto es, $\mathcal{A}$ es no válido e, igualmente, la correspondiente argumentación es no válida.

3. *Identificación de los modelos que proporcionan las ramas satisfactibles.*

La rama satisfactible ρ_1 proporciona un modelo para Γ, a saber, la interpretación $I(p) = 1, I(q) = 0$, la cual es un contramodelo para $(p \vee q) \wedge p \to q$, la expresión en lógica de juntores de la deducción semántica $\{p \vee q, p\} \vDash q$.

4. *Demostración de que los modelos lo son para Γ.*

No es difícil demostrar que I_{10} es un modelo para Γ; para ello, estudiemos la valoración de verdad de las fórmulas de Γ con dicha interpretación:

p	q	p	∨	q	p	¬	q
1	0	1	[1]	0	[1]	[1]	0

5. *Expresión en español de las contraargumentaciones construidas a partir de los modelos.*

   Contraargumentar $\{\phi_0, \phi_1\} \vDash \psi$ es satisfacer $(\phi_0 \land \phi_1) \land \neg\psi$.

   De esta manera, refutamos la afirmación propuesta: que se satisfaga p y no se satisfaga q es suficiente para que no se satisfaga dicha afirmación; en otras palabras, se satisfacen ambas premisas (la primera porque como se satisface p, da igual que se satisfaga q o no, la disyunción se satisface; la segunda porque se satisface p), pero no se satisface la conclusión (porque no se satisface q). ■

Ejemplo 155

> «Las IA (inteligencias artificiales) manejan creencias, pero una multitud de IA no es caótica, sino que está organizada colectivamente. De hecho, si una multitud de IA se organiza colectivamente y no es caótica, es porque las IA manejan creencias. Por tanto, puede concluirse que una multitud de IA no se organizará colectivamente siempre que no haya IA que manejen creencias».
>
> ---
>
> [EFO 3.6.2019:1], [EFO 3.6.2019:1b1] (por tablas semánticas).

Resolución.— En el ejemplo 135 (pág. 226 de esta edición) resolvimos esta argumentación por reducción al absurdo (Abs, RAA).

0. y 1. En dicho ejemplo resolvimos los apartados 0 y 1 que aquí se piden, esto es, allí: 0.º, hallamos el argumento $\mathcal{A}$ correspondiente; 1.º, propusimos su formalización (variables proposicionales, esquema argumental y forma lógica) en lógica de juntores; 2.º, identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{p \land \neg q \land r, p \rightarrow (r \land \neg q)\}$ y la conclusión ψ, a saber, $\neg p \rightarrow \neg r$, y 3.º, sugerimos la forma lógica en lógica de juntores para $\mathcal{A}$, que resultó ser $(p \land \neg q \land r) \land (p \rightarrow (r \land \neg q)) \rightarrow (\neg p \rightarrow \neg r)$.

   Ahora nos preguntamos si $(p \land \neg q \land r) \land (p \rightarrow (r \land \neg q)) \rightarrow (\neg p \rightarrow \neg r)$ es una fórmula válida, esto es, si $\vDash (p \land \neg q \land r) \land (p \rightarrow (r \land \neg q)) \rightarrow (\neg p \rightarrow \neg r)$.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

   1. *Identificación del conjunto* Γ.

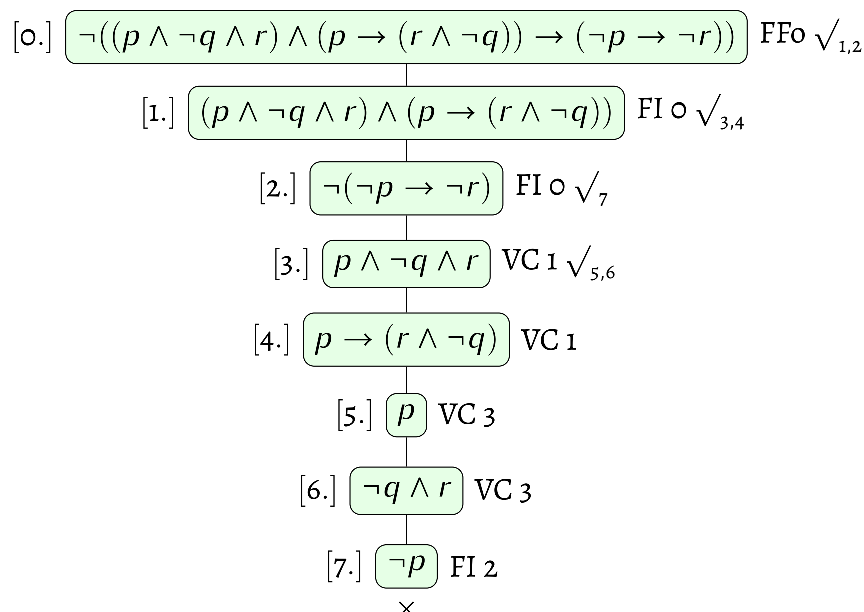
      De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con ser $\phi_0 \land \phi_1 \rightarrow \psi$ una fórmula válida, esto es, con $\vDash \phi_0 \land \phi_1 \rightarrow \psi$. Refutar $\vDash \phi_0 \land \phi_1 \rightarrow \psi$ es demostrar que $(\phi_0 \land \phi_1) \land \neg\psi$ es una fórmula válida.

      Definimos $\Gamma = \{\neg((p \land \neg q \land r) \land (p \rightarrow (r \land \neg q)) \rightarrow (\neg p \rightarrow \neg r))\}$.

Estudiemos si existe una refutación para Γ —esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible—, un árbol de refutación, para Γ.

II. *Construcción anotada del árbol semántico.*

Sea el árbol:



Observación.— FF0 $\leftrightharpoons$ Falsedad de la fórmula; FI $\leftrightharpoons$ Falsedad de la implicación; VC $\leftrightharpoons$ Verdad de la conjunción.

III. *Demostración de que es un árbol terminado.*

Este árbol de refutación tiene una rama:

$\rho_0 = \langle((p \land \neg q \land r) \land (p \to (r \land \neg q))) \to (\neg p \to \neg r), (p \land \neg q \land r) \land (p \to (r \land \neg q)), \neg(\neg p \to \neg r), p \land (\neg q \land r), p \to (r \land \neg q), p, (\neg q \land r), \neg p, \neg\neg r\rangle$.

Es un árbol terminado (toda rama es insatisfactible o completa), pues ρ_0 es insatisfactible, al existir en ella una variable y su negación: p (nodo 5) y $\neg p$ (nodo 7).

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como la única rama es insatisfactible, este árbol terminado es insatisfactible, por lo que hemos demostrado que Γ es un conjunto insatisfactible de fórmulas, en otras palabras, hemos demostrado que existe una refutación para Γ (traducido a $\mathcal{L}_0$, para $\phi_0 \land \phi_1 \land \neg\psi$), lo cual, por el teorema 3.8 (pág. 281 de esta edición), equivale a haber demostrado $\models \phi_0 \land \phi_1 \to \psi$, es decir, en este ejemplo, a que $(p \land \neg q \land r) \land (p \to (r \land \neg q)) \to (\neg p \to \neg r)$ es una fórmula válida, en otras palabras, a que el argumento $\mathcal{A}$ es válido e, igualmente, a que es válida la argumentación correspondiente.

3. No procede (no hay ramas satisfactibles).

4. No procede (no hay modelos para Γ).

5. No procede (no hay contraargumentaciones). ■

Ejemplo 156

> «Las personas colaboran cuando cooperan, pero no es cierto que cooperen si colaboran. Que las personas cooperen significa que se apoyan mutuamente. En definitiva, las personas se apoyan mutuamente siempre que cooperan aunque no colaboren».
>
> ---
>
> [EFE 25.6.2019:1b1] (por tablas semánticas).

Resolución.— En el ejemplo 135 (pág. 226 de esta edición) resolvimos esta argumentación por reducción al absurdo (Abs, RAA).

0. y 1. En dicho ejemplo resolvimos los apartados 0 y 1 que aquí se piden, esto es, allí: 0.º, hallamos el argumento $\mathcal{A}$ correspondiente; 1.º, propusimos su formalización (variables proposicionales, esquema argumental y forma lógica) en lógica de juntores; 2.º, identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{(p \to q), \neg(q \to p)\}$ y la conclusión ψ, a saber, $p \to r$, y 3.º, sugerimos la forma lógica en lógica de juntores para $\mathcal{A}$, que resultó ser $(p \to q) \land \neg(q \to p) \land (p \leftrightarrow r) \to (p \to r)$.

   Ahora nos preguntamos si $(p \to q) \land \neg(q \to p) \land (p \leftrightarrow r) \to (p \to r)$, es una fórmula válida, en otras palabras, si se satisface $\vDash (p \to q) \land \neg(q \to p) \land (p \leftrightarrow r) \to (p \to r)$.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

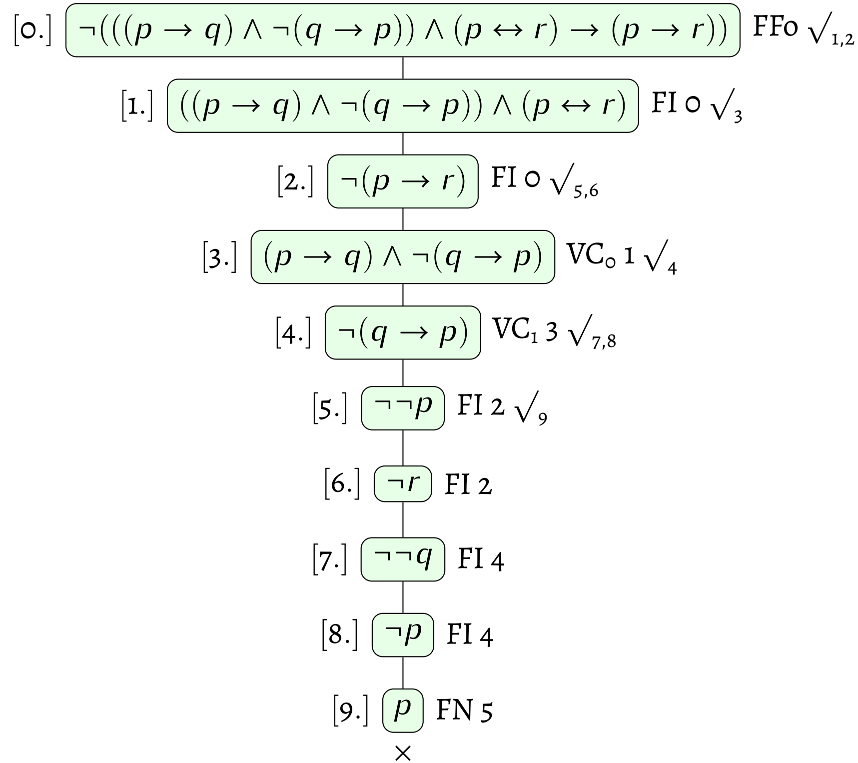
   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con ser $\phi_0 \land \phi_1 \to \psi$ una fórmula válida, esto es, con $\vDash \phi_0 \land \phi_1 \to \psi$. Refutar $\vDash \phi_0 \land \phi_1 \to \psi$ es demostrar que $(\phi_0 \land \phi_1) \land \neg\psi$ es una fórmula válida.

   Definimos $\Gamma = \{\neg((p \to q) \land \neg(q \to p) \land (p \leftrightarrow r) \to (p \to r))\}$. Estudiemos si existe una refutación para Γ —esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible—, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico.*

   Sea el árbol:



Observación.— FFo $\leftrightharpoons$ Falsedad de la fórmula; FI $\leftrightharpoons$ Falsedad de la implicación; FN $\leftrightharpoons$ Falsedad de la negación; VC $\leftrightharpoons$ Verdad de la conjunción.

III. *Demostración de que es un árbol terminado.*

Este árbol de refutación tiene una rama:

$\rho_0 = \langle \neg((((p \to q) \land \neg(q \to p)) \land (p \leftrightarrow r)) \to (p \to r)), (((p \to q) \land \neg(q \to p)) \land (p \leftrightarrow r), \neg(p \to r), ((p \to q) \land \neg(q \to p)), (p \leftrightarrow r), (p \to q), \neg(q \to p), p, \neg r, q, \neg p \rangle$.

Es un árbol terminado (toda rama es insatisfactible o completa), pues ρ_0 es insatisfactible, al existir en ella una variable y su negación: p (nodo 9) y $\neg p$ (nodo 8).

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como la única rama es insatisfactible, este árbol terminado es insatisfactible, por lo que hemos demostrado que Γ es un conjunto insatisfactible de fórmulas, en otras palabras, hemos demostrado que existe una refutación para Γ (traducido a $\mathcal{L}_0$, para $\phi_0 \land \phi_1 \land \neg\psi$), lo cual, por el teorema 3.8 (pág. 281 de esta edición), equivale a haber demostrado $\vDash \phi_0 \land \phi_1 \to \psi$, es decir, en este ejemplo, a que $((p \to q) \land \neg(q \to p)) \land (p \leftrightarrow r) \to (p \to r)$ es una fórmula válida, en otras palabras, a que el argumento $\mathcal{A}$ es válido e, igualmente, a que es válida la argumentación correspondiente.

3. No procede (no hay ramas satisfactibles).

4. No procede (no hay modelos para Γ).

5. No procede (no hay contraargumentaciones). ■

Ejemplo 157

«En Tierrapésima, se ha comprobado que siempre que una solución es beneficiosa para la ciudadanía, pero es perjudicial para el bolsillo de la dirigencia política, entonces habrá dirigentes políticos que harán todo lo posible porque no se adopte, esto es, por prevaricar». ¿Se deduce de aquí que, en Tierrapésima, cuando una solución es beneficiosa para la ciudadanía, entonces, si ocurre que es perjudicial para el bolsillo de la dirigencia política, entonces habrá dirigentes políticos que harán todo lo posible porque no se adopte, esto es por prevaricar? ¿Reconocemos alguna regla deductiva estudiada?

[SEL 3:3].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si una solución es beneficiosa para la ciudadanía y es perjudicial para el bolsillo de la dirigencia política, entonces hay dirigentes políticos que harán todo lo posible porque no se adopte, esto es, por prevaricar. Luego, si una solución es beneficiosa para la ciudadanía, entonces de suponer que una solución es perjudicial para el bolsillo de la dirigencia política, se sigue que hay dirigentes políticos harán todo lo posible porque no se adopte, esto es, por prevaricar.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

- *Variables proposicionales*:

  Siendo el universo de discurso el conjunto de todas las personas, consideremos las siguientes variables proposicionales y las proposiciones simples que representan:

  $p \fallingdotseq$ una solución es beneficiosa para la ciudadanía;

  $q \fallingdotseq$ una solución es perjudicial para el bolsillo de la dirigencia política;

  $r \fallingdotseq$ hay dirigentes políticos que harán todo lo posible porque no se adopte, esto es, por prevaricar.

- *Esquema argumental*:

  Si se supone p y q, se sigue r.
  ∴ Se sigue que si se supone p, se sigue que si se supone q, se sigue r.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0\} = \{(p \wedge q) \to r\}$, con una única premisa, y la conclusión ψ, a saber, $p \to (q \to r)$.

La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $((p \wedge q) \rightarrow r) \rightarrow (p \rightarrow (q \rightarrow r))$; llamémosla A.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

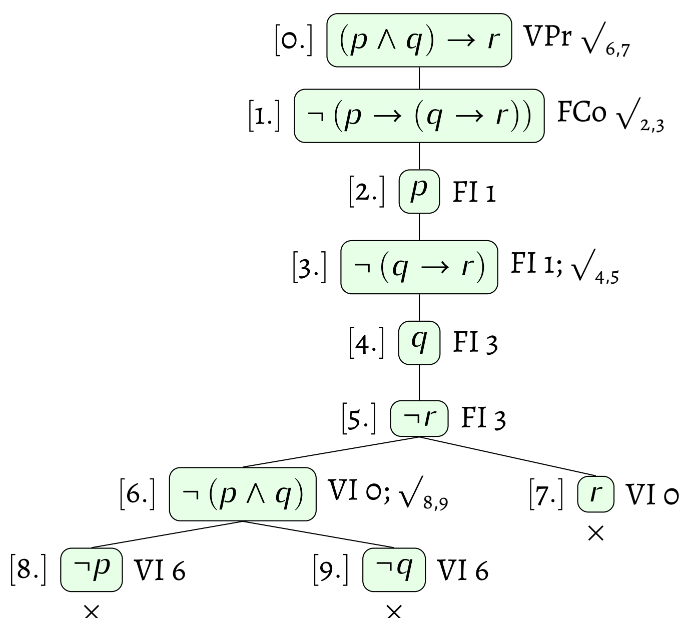
Reconocemos la regla deductiva de inferencia, $\Phi \vdash \psi$, *ley de exportación*[31], $\{(p \wedge q) \rightarrow r\} \vdash p \rightarrow (q \rightarrow r)$. Demostremos que efectivamente es una regla deductiva. Para ello, aplicaremos TA/S a su contraparte semántica, la deducción semántica $\{(p \wedge q) \rightarrow r\} \vDash p \rightarrow (q \rightarrow r)$, en otras palabras, analicemos si $p \rightarrow (q \rightarrow r)$ es consecuencia lógica del conjunto unitario de fórmulas $\{(p \wedge q) \rightarrow r\}$.

I. *Identificación del conjunto* Γ.

De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283 de esta edición), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0\} \vDash \psi$. Refutar $\{\phi_0\} \vDash \psi$ es demostrar que $\phi_0 \wedge \neg\psi$ es una fórmula válida.

Definimos $\Gamma = \{(p \wedge q) \rightarrow r, \neg(p \rightarrow (q \rightarrow r))\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

II. *Construcción anotada del árbol semántico.*



Observación.— VPr ⥱ Verdad de la premisa; FCo ⥱ Falsedad de la conclusión; FI ⥱ Falsedad de la implicación; VI ⥱ Verdad de la implicación.

III. *Demostración de que es un árbol terminado.*

[31] *Cfr. supra* teorema 2.16 (pág. 203 de esta edición).

Hemos de demostrar que toda rama es insatisfactible o completa. Este árbol semántico tiene un tronco ρ_0 y tres ramas ρ_1, ρ_2 y ρ_3:

$$\begin{aligned}
\rho_0 &= \langle (p \wedge q) \to r, \neg (p \to (q \to r)), p, \neg (q \to r), q, \neg r \rangle, \\
\rho_1 &= \rho_0 +\!\!+ \langle \neg (p \wedge q), \neg p \rangle, \\
\rho_2 &= \rho_0 +\!\!+ \langle \neg (p \wedge q), \neg q \rangle, \\
\rho_3 &= \rho_0 +\!\!+ \langle r \rangle.
\end{aligned}$$

Las tres ramas son insatisfactibles:

- la rama ρ_1 ya que aparecen p (nodo 2) y $\neg p$ (nodo 8);
- la rama ρ_2 pues aparecen q (nodo 4) y $\neg q$ (nodo 9), y
- la rama ρ_3 dado que aparecen $\neg r$ (nodo 5) y r (nodo 7).

Concluimos que se trata de un árbol terminado insatisfactible.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como este árbol terminado es insatisfactible, hemos encontrado una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), $p \to (q \to r)$ es consecuencia lógica del conjunto unitario de fórmulas $\{(p \wedge q) \to r\}$, esto es, el argumento $\mathcal{A}$ es válido e, igualmente, lo es la correspondiente argumentación.

3. No procede (no hay ramas satisfactibles).
4. No procede (no hay modelos para Γ).
5. No procede (no hay contraargumentaciones). ■

Ejemplo 158

«Si vas tú, viene Ángela. Si no vas tú, viene Micaela. Por tanto, si viene Micaela, no viene Ángela».

[Cubit 35], [EFE 28.6.2023:1], [EFO 27.5.2025:1], [EFE 18.6.2025:1], [SEL 3:7].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si vas tú, entonces viene Ángela. Si no vas tú, entonces viene Micaela. Luego, si viene Micaela, entonces no viene Ángela.

Que reescrito destacando los juntores (recuadrados) y el deductor (subrayado) es:

De tener que [si] vas tú, [entonces] viene Ángela, y que [si] [no] vas tú, [entonces] viene Micaela, se sigue que [si] viene Micaela, [entonces] [no] viene Ángela.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales.*

     Siendo el universo de discurso el conjunto de todas las personas, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

     $$g \leftrightharpoons \text{viene Ángela}, \qquad m \leftrightharpoons \text{viene Micaela}, \qquad t \leftrightharpoons \text{vas tú}.$$

   - *Esquema argumental*:

     Si se supone t, se sigue g.
     Si se supone no t, se sigue m.
     ∴ Se sigue que si se supone m, se sigue no g.

   - *Forma lógica.*

     Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{t \to g, \neg t \to m\}$, con una única premisa, y la conclusión ψ, a saber, $m \to \neg g$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(t \to g) \wedge (\neg t \to m) \to (m \to \neg g)$; llamémosla A.

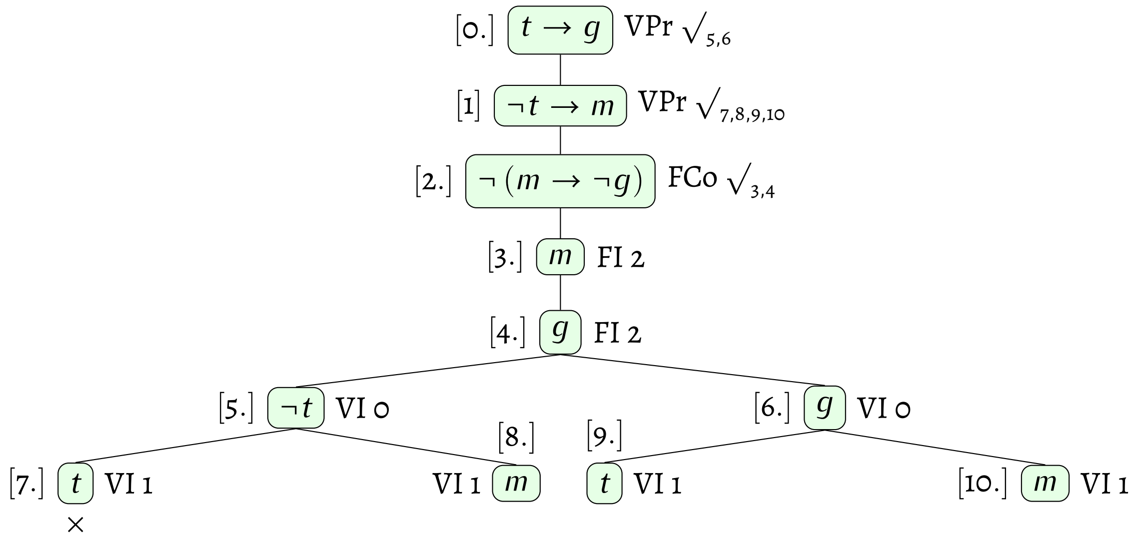
2. *Demostración de la no validez de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1\} \vDash \psi$. Refutar $\{\phi_0, \phi_1\} \vDash \psi$ es demostrar que $\phi_0 \wedge \neg\psi$ es una fórmula válida. Definimos $\Gamma = \{t \to g, \neg t \to m, \neg(m \to \neg g)\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico.*

   Sea el árbol



Observación.— VPr ⥫ Verdad de la premisa; FCo ⥫ Falsedad de la conclusión; FI ⥫ Falsedad de la implicación; VI ⥫ Verdad de la implicación.

III. *Demostración de que es un árbol terminado*.

Este árbol consta de su tronco $\rho_0 = \langle t \to g, \neg t \to m, \neg(m \to \neg g), m, g\rangle$ y sus cuatro ramas,

$$\rho_1 = \rho_0 + \langle \neg t, t\rangle = \langle t \to g, \neg t \to m, \neg(m \to \neg g), m, g, \neg t, t\rangle,$$
$$\rho_2 = \rho_0 + \langle \neg t, m\rangle = \langle t \to g, \neg t \to m, \neg(m \to \neg g), m, g, \neg t, m\rangle,$$
$$\rho_3 = \rho_0 + \langle g, t\rangle = \langle t \to g, \neg t \to m, \neg(m \to \neg g), m, g, g, t\rangle,$$
$$\rho_4 = \rho_0 + \langle g, m\rangle = \langle t \to g, \neg t \to m, \neg(m \to \neg g), m, g, g, m\rangle.$$

Es un árbol terminado, pues toda rama es insatisfactible o completa.

En efecto:

a. ρ_1 es insatisfactible, pues incluye una variable y su negación: t y $\neg t$;

b. ρ_2, ρ_3 y ρ_4 son ramas satisfactibles (ya que como se verá en el apartado 3, existen modelos para cada rama $\rho \in \{\rho_2, \rho_3, \rho_4\}$, precisamente los modelos que proporciona ρ para Γ), aunque completas:

- ρ_2 es completa, pues en ρ_2: estando $t \to g$, está $\neg t$ o g (están ambas); estando $\neg t \to m$, está t o m (está m), y estando $\neg(m \to \neg g)$, está m y g;
- ρ_3 es completa, porque en ρ_3: estando $t \to g$, está $\neg t$ o g (está g); estando $\neg t \to m$, está t o m (están ambas), y estando $\neg(m \to \neg g)$, está m y g;
- ρ_4 es completa, ya que en ρ_4: estando $t \to g$, está $\neg t$ o g (está g); estando $\neg t \to m$, está t o m (está m), y estando $\neg(m \to \neg g)$, está m y g.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existen ramas satisfactibles, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), de $t \to g$ y $\neg t \to m$ no se sigue $m \to \neg g$, esto es, el argumento $\mathcal{A}$ no es válido e, igualmente, tampoco es válida la argumentación correspondiente.

3. *Identificación de los modelos para Γ que proporcionan las ramas satisfactibles.*

Al ser ρ_2, ρ_3 y ρ_4 ramas satisfactibles, proporcionan modelos para Γ, a saber,

- ρ_2 proporciona $I(g) = 1$, $I(m) = 1$ e $I(t) = 0$, abreviadamente, I_{110};
- ρ_3 proporciona $I(g) = 1$, $I(m) = 1$ e $I(t) = 1$, abreviadamente, I_{111};
- ρ_4 proporciona $I(g) = 1$, $I(m) = 1$ e $I(t) = 0$, abreviadamente, I_{110}, e $I(g) = 1$, $I(m) = 1$ e $I(t) = 1$, abreviadamente, I_{111}.

En definitiva, las interpretaciones I_{111} e I_{110} son los únicos modelos para Γ.

4. *Demostración de que los modelos lo son para Γ.*

No es difícil demostrar que I_{111} e I_{110} son modelos para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dichas interpretaciones:

g	m	t	t	$\to$	g	$\neg$	t	$\to$	m	$\neg$	(	m	$\to$	$\neg$	g	)
1	1	1	1	$\boxed{1}$	1	0	1	$\boxed{1}$	1	$\boxed{1}$		1	0	0	1	
1	1	0	0	$\boxed{1}$	1	1	0	$\boxed{1}$	1	$\boxed{1}$		1	0	0	1	

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

Contraargumentar $\{\phi_0, \phi_1\} \vDash \psi$ es satisfacer $(\phi_0 \wedge \phi_1) \wedge \neg\psi$.

De esta manera, refutamos la afirmación propuesta: que vayan Ángela y Micaela es suficiente para que no se satisfaga dicha afirmación; en otras palabras, se satisfacen ambas premisas (la primera porque como viene Ángela, da igual que vengas tú o no, ella viene; la segunda porque como viene Micaela, da igual que vengas tú o no, ella viene), pero no se satisface la conclusión (porque viene Micaela y viene Ángela). ■

Observación 3.3.6.— Si hubiésemos reducido $(t \to g) \wedge (\neg t \to m) \to (m \to \neg g)$ a su forma normal disyuntiva, habríamos visto que ésta es $\neg g \vee \neg m$, equivalente a $\neg(g \wedge m)$, una contingencia cuya refutación equivale a ser verdad g y m (pudiendo t ser verdad o no), esto es, precisamente los modelos que habíamos descubierto.

Observación 3.3.7.— Recordemos: las expresiones *rama cerrada* y *rama abierta* pertenecen a la sintaxis; en la semántica, sus correspondientes son *rama insatisfactible* y *rama satisfactible*.

Observación 3.3.8.— Los signos ⊨ (deductor semántico) y ⁂ (asterismo) no son propios de la lógica sino de la metalógica.

Observación 3.3.9.— El argumento «Si vas tú, viene Ángela. Si no vas tú, viene Micaela. Por lo tanto, si no viene Micaela, viene Ángela.» es válido.

Ejemplo 159

«Dos personas no se pelean si una no quiere. De hecho, se pelean sólo si una tercera persona interviene. Por tanto, dos personas no se pelean a menos que las dos quieran o una tercera persona intervenga».

[EFEC 25.6.2019:1], [EFO 4.6.2021:1].

Resolución.—

0. *Argumento*.

   Reescritura de la argumentación.

   Reescribiendo la argumentación para intentar aclarar su significado además de para acercarlo a patrones más sencillos de traducción de los conectores de la lógica de juntores, identificando las premisas y la conclusión:

   Si no sucede que dos personas quieran pelearse, entonces no sucede que (las) dos personas se pelean [Premisa 0]. Si (las dos) se pelean, entonces (es que) interviene una tercera persona [Premisa 1]. Por tanto, si no sucede que las dos quieran pelearse y tampoco que una tercera intervenga, entonces no sucede que (las dos) se pelean [Conclusión].

   Argumento ($\mathcal{A}$): Si es falso que dos personas quieran pelearse, entonces no se pelean. Si se pelean, entonces interviene una tercera persona. Si dos personas no quieren pelearse y no interviene una tercera persona, entonces, las dos personas no se pelean.

   Validez intuitiva.

   Intuitivamente, parece válido, pues el antecedente de la conclusión es la conjunción del antecedente de la primera premisa y del antecedente de la contrarrecíproca de la segunda premisa, siendo ambos consecuentes el mismo, a saber, el consecuente de la conclusión.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

   - *Variables proposicionales*:

Siendo el universo de discurso el conjunto de todas las personas, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

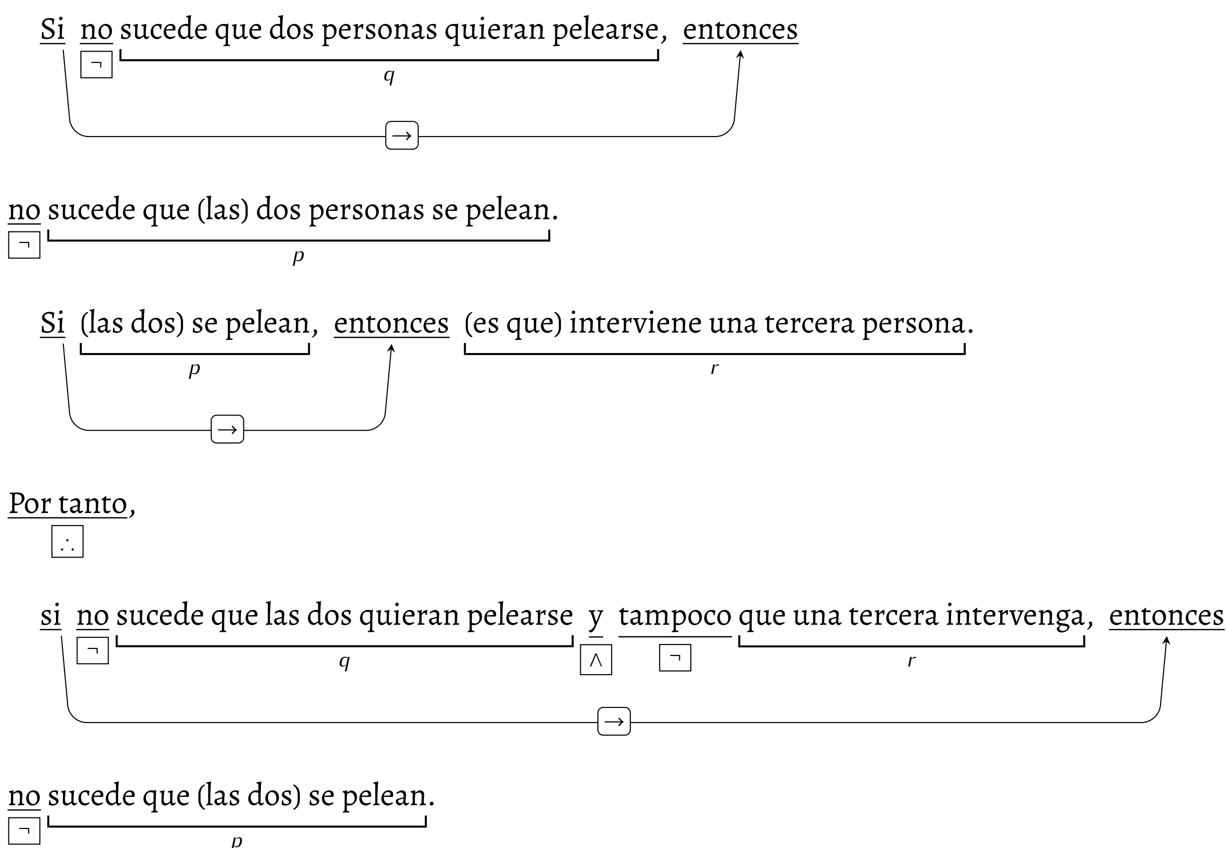
$$p \leftrightharpoons \text{(las) dos personas se pelean;}$$
$$q \leftrightharpoons \text{(las) dos personas quieren pelearse;}$$
$$r \leftrightharpoons \text{una tercera persona interviene.}$$

- *Esquema argumental*.

  Estructura lógico-gramatical.

  En $\mathcal{A}$ identificamos dos oraciones enunciativas como premisas y una tercera como conclusión (pues ésta está precedida de «Por tanto», un indicador de conclusión, esto es, apunta que el enunciado que sigue es la conclusión del argumento).

  Subrayemos ahora las conectivas e identifiquemos las proposiciones simples.



  Observemos que el indicador de conclusión «Por tanto» queda designado por la conectiva ∴ del metalenguaje.

Esquema argumental:

$$\begin{array}{rl} & \text{Si se supone no } q\text{, se sigue no } p. \\ & \text{Si se supone } p\text{, se sigue } r. \\ \hline \therefore & \text{Se sigue que si se supone no } q \text{ y no } r\text{, se sigue no } p. \end{array} \tag{3.4}$$

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{\neg q \to \neg p, p \to r\}$, con una única premisa, y la conclusión ψ, a saber, $(\neg q \wedge \neg r) \to \neg p$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(\neg q \to \neg p) \wedge (p \to r) \to ((\neg q \wedge \neg r) \to \neg p)$. Llamémosla A.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos*.

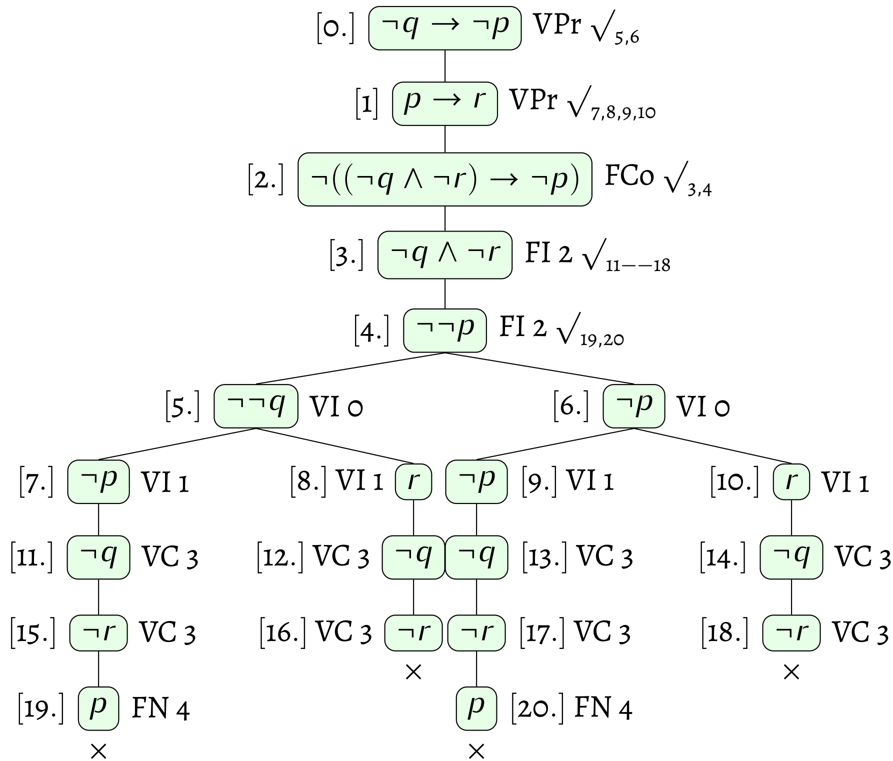
   I. *Identificación del conjunto* Γ.

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1\} \vDash \psi$. Refutar $\{\phi_0, \phi_1\} \vDash \psi$ es demostrar que $\phi_0 \wedge \phi_1 \wedge \neg\psi$ es una fórmula válida.

   Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0, \phi_1\} \cup \{\neg\psi\} = \{\neg q \to \neg p, p \to r, \neg((\neg q \wedge \neg r) \to \neg p)\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico*.

   Sea el árbol:



Observación.— VPr ⥱ Verdad de la premisa; FCo ⥱ Falsedad de la conclusión; FI ⥱ Falsedad de la implicación; FN ⥱ Falsedad de la negación; VC ⥱ Verdad de la conjunción; VI ⥱ Verdad de la implicación.

III. *Demostración de que es un árbol terminado.*

Este árbol de refutación tiene cuatro ramas.

Designando por ρ_0 el conjunto de nodos iniciales comunes (tronco),

$$\rho_0 = \langle \neg q \to \neg p, p \to r, \neg((\neg q \land \neg r) \to \neg p), \neg q \land \neg r, \neg\neg p \rangle,$$

las cuatro ramas son:

$$\begin{aligned} \rho_1 &= \rho_0 +\!\!+ \langle \neg\neg q, \neg p, \neg q, \neg r, p \rangle, \\ \rho_2 &= \rho_0 +\!\!+ \langle \neg\neg q, r, \neg q, \neg r \rangle, \\ \rho_3 &= \rho_0 +\!\!+ \langle \neg p, \neg p, \neg q, \neg r, p \rangle, \\ \rho_4 &= \rho_0 +\!\!+ \langle \neg p, r, \neg q, \neg r \rangle. \end{aligned}$$

Es un árbol terminado, pues toda rama es insatisfactible al existir en cada una de ellas al menos una variable y su negación: p y $\neg p$ en ρ_1 y ρ_3, y r y $\neg r$ en ρ_2 y ρ_4.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como todas las ramas son insatisfactibles, este árbol terminado es insatisfactible, por lo que Γ es un conjunto insatisfactible de fórmulas, en otras palabras, hemos demostrado que existe una refutación para $\Gamma = \{\phi_0, \phi_1\} \cup \{\neg\psi\}$ (traducido a $\mathcal{L}_0$, para $\phi_0 \wedge \phi_1 \wedge \neg\psi$), lo cual, por el teorema 3.8 (pág. 281 de esta edición), equivale a haber demostrado $\phi_0 \wedge \phi_1 \vDash \psi$, es decir, en este ejemplo, a que $\neg q \wedge \neg r \rightarrow \neg p$ es consecuencia lógica de $(\neg q \rightarrow \neg p) \wedge (p \rightarrow r)$, en otras palabras, a que el argumento $\mathcal{A}$ es válido e, igualmente, a que es válida la argumentación correspondiente.

3. No procede (no hay ramas satisfactibles).

4. No procede (no hay modelos para Γ).

5. No procede (no hay contraargumentaciones). ■

Observación 3.3.10.— Llamando A y B a las dos personas, pudiésemos haber reescrito q como $q_A \wedge q_B$ haciendo referencia explícita a ambas; en este caso, el esquema argumental (3.4) es

Si se supone no (q_A y q_B), se sigue no p.
Si se supone p, se sigue r.

∴ Se sigue que si se supone no (q_A y q_B) y no r, se sigue no p.

Observación 3.3.11.— Alternativamente, una vez formalizado pudiésemos haber simplificado las fórmulas mediante equivalencias lógicas, de manera que el esquema argumental (3.4) se simplifica en

Si se supone p, se sigue q.
Si se supone p, se sigue r.

∴ Se sigue que si se supone p, se sigue q o r.

Ejemplo 160

«De tres jugadores, A, B y C, se sabe sólo que "C miente siempre que miente A" o que "la mentira de B siempre es seguida de la mentira de C". Por lo tanto, se deduce que "si A o B mienten, entonces C miente"».

[PEP 10.4.2019:1], [EFE 19.1.2023:1], [EFO 24.5.2023:1], [EFE 3.7.2024:1] (tipo test), [EFE 29.1.2025:1] (tipo test) (tres servidores que fallan), [EFEC 29.1.2025:1] (tipo test) (tres sistemas que se reinician).

Resolución.—

0. *Argumento.*

- *Reescritura de la argumentación.*

La hipótesis es una disyunción. Reescribimos, por una parte, el primer disyunto, «C miente siempre que miente A», de manera equivalente, como «siempre que miente A, miente

C», y, en definitiva, «si miente A, entonces miente C», y, por otra, el segundo disyunto, «la mentira de B siempre es seguida de la mentira de C», como «la mentira de B tiene como consecuencia la mentira de C» y, en definitiva, como «si miente B, entonces miente C».

- *Argumento* ($\mathcal{A}$): O bien sucede que si la persona A miente, entonces la persona C miente, o bien que si la persona B miente, entonces la persona C miente, o bien, quizás, pudiesen suceder ambas cosas. Luego, si la persona A miente o la persona B miente, o ambas mienten, entonces la persona C miente.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

   - *Variables proposicionales*.

     Siendo el universo de discurso el conjunto de todas las personas, consideramos tres variables proposicionales y las proposiciones simples que representan (con la licencia de designar a aquéllas como a éstas, con letras latinas mayúsculas):

     $A \leftrightharpoons A$ miente; $B \leftrightharpoons B$ miente; $C \leftrightharpoons C$ miente.

   - *Esquema argumental*:

     Si se supone que,
     bien si se supone A, se sigue C,
     bien si se supone B, se sigue C,
     bien ambas.
     ∴ Se sigue que si se supone A o B o ambas, se sigue C.

   - *Forma lógica*.

     Identificamos el conjunto de premisas $\Phi = \{\phi_0\} = \{(A \to C) \vee (B \to C)\}$, con una única premisa, y la conclusión ψ, a saber, $A \vee B \to C$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(A \to C) \vee (B \to C) \to (A \vee B \to C)$. Llamémosla A.

     Observación.— Pudiésemos trabajar con cualquier otra fórmula lógicamente equivalente, por ejemplo, $((A \to C) \vee (B \to C)) \wedge (A \vee B) \to C$.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos*.

   1. *Identificación del conjunto* Γ.

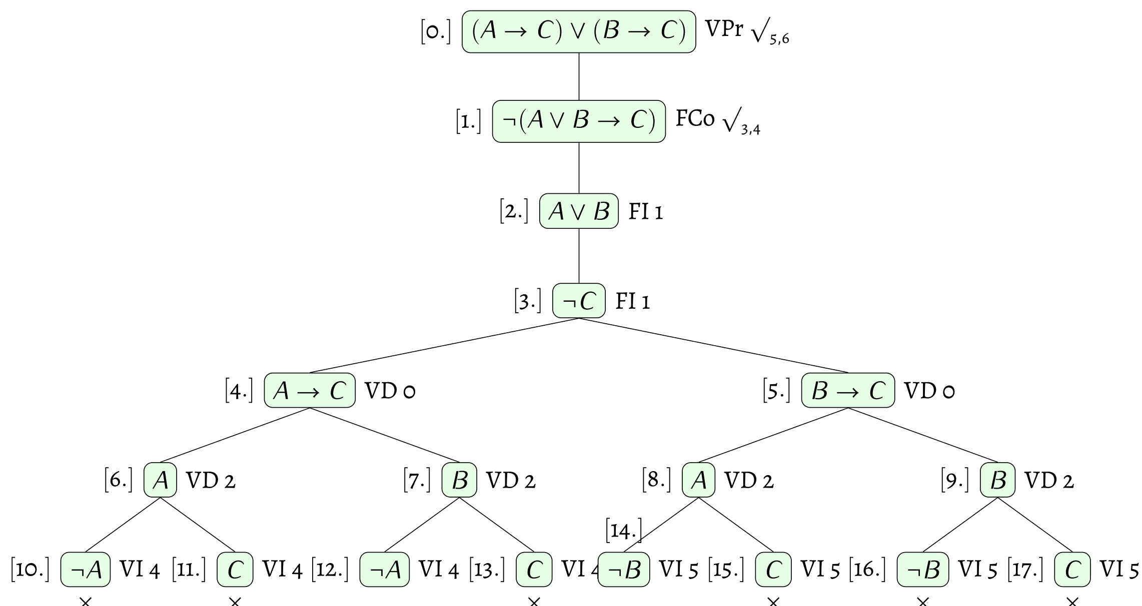
      De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0\} \vDash \psi$. Refutar $\{\phi_0\} \vDash \psi$ es demostrar que $\phi_0 \wedge \neg\psi$ es una fórmula válida.

      Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0\} \cup \{\neg\psi\} = \{(A \to C) \vee (B \to C), \neg(A \vee B \to C)\}$. Estudiemos si existe una refutación para Γ, esto

es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

II. *Construcción anotada del árbol semántico.*

Sea el árbol:



Observación.— VPr $\leftrightharpoons$ Verdad de la premisa; FCo $\leftrightharpoons$ Falsedad de la conclusión; FI $\leftrightharpoons$ Falsedad de la implicación; VD $\leftrightharpoons$ Verdad de la disyunción; VI $\leftrightharpoons$ Verdad de la implicación.

III. *Demostración de que es un árbol terminado.*

Este árbol tiene un tronco, $\rho_0 = \langle\ (A \to C) \vee (B \to C),\ \neg((A \vee B) \to C),\ A \vee B,\ \neg C\rangle$, y ocho ramas, a saber,

$\rho_1 = \rho_0 +\!\!+ \langle A \to C), A, \neg A\rangle,$ $\rho_5 = \rho_0 +\!\!+ \langle B \to C), A, \neg B\rangle,$
$\rho_2 = \rho_0 +\!\!+ \langle A \to C), A, C\rangle,$ $\rho_6 = \rho_0 +\!\!+ \langle B \to C), A, C\rangle,$
$\rho_3 = \rho_0 +\!\!+ \langle A \to C), B, \neg A\rangle,$ $\rho_7 = \rho_0 +\!\!+ \langle B \to C), B, \neg B\rangle,$
$\rho_4 = \rho_0 +\!\!+ \langle A \to C), B, C\rangle,$ $\rho_8 = \rho_0 +\!\!+ \langle B \to C), B, C\rangle.$

Es un árbol terminado, pues toda rama es insatisfactible o completa; en efecto, por una parte,

- ρ_1 es insatisfactible ($A, \neg A \in \rho_1$),
- ρ_2 es insatisfactible ($C, \neg C \in \rho_2$),
- ρ_4 es insatisfactible ($C, \neg C \in \rho_4$),
- ρ_6 es insatisfactible ($C, \neg C \in \rho_6$),
- ρ_7 es insatisfactible ($B, \neg B \in \rho_7$),
- ρ_8 es insatisfactible ($C, \neg C \in \rho_8$),

y, por otra, ρ_3 y ρ_5 no son insatisfactibles aunque sí son completas:

- ρ_3 porque:
  - está [0] $(A \to C) \vee (B \to C)$ y el disyunto [4] $A \to C$,
  - está [1] $\neg(A \vee B \to C)$ y los conjuntos [2] $A \vee B$ y [3] $\neg C$,
  - está [2] $A \vee B$ y el disyunto [7] B, y
  - está [4] $A \to C$ y el disyunto [12] $\neg A$, y
- ρ_5 porque
  - está [0] $(A \to C) \vee (B \to C)$ y el disyunto [5] $B \to C$,
  - está [1] $\neg(A \vee B \to C)$ y los conjuntos [2] $A \vee B$ y [3] $\neg C$,
  - está [2] $A \vee B$ y el disyunto [8] A, y
  - está [5] $B \to C$ y el disyunto [14] $\neg B$.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existen dos ramas satisfactibles, ρ_3 y ρ_5, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), de $(A \to C) \vee (B \to C)$ no se deduce $A \vee B \to C$, esto es, el argumento $\mathcal{A}$ no es válido e, igualmente, tampoco es válida la argumentación correspondiente.

3. *Identificación de los modelos que proporcionan las ramas satisfactibles.*

Al ser ρ_3 y ρ_5 ramas satisfactibles, proporcionan modelos para el conjunto de fórmulas bien formadas Γ, a saber:

I. ρ_3 proporciona: $I(A) = 0$, $I(B) = 1$ e $I(C) = 0$, abreviadamente, I_{010};

II. ρ_5 proporciona: $I(A) = 1$, $I(B) = 0$ e $I(C) = 0$, abreviadamente, I_{100}.

En definitiva, las interpretaciones I_{100} e I_{010} son los únicos modelos para Γ.

4. *Demostración de que los modelos lo son para Γ.*

No es difícil demostrar que I_{100} e I_{010} son modelos para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dichas interpretaciones:

A	B	C	(	A	→	C	)	∨	(	B	→	C	)	¬	(	A	∨	B	→	C	)
1	0	0		1	0	0		[1]		0	1	0		[1]		1	1	0	0	0	
0	1	0		0	1	0		[1]		1	0	0		[1]		0	1	1	0	0	

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

Ejemplos de contrargumentos para refutar $\mathcal{A}$ son:

I. (a partir de I_{100}) que A mienta y B y C no, es suficiente para que no se satisfaga el argumento, ya que se satisface que la mentira de B siempre es seguida de la mentira de C, pero no se satisface la conclusión, pues A miente y C no miente;

II. (a partir de I_{010}) que B mienta y A y C no, es suficiente para que no se satisfaga el argumento, ya que se satisface que "C miente siempre que miente A", pero no se satisface la conclusión, pues B miente y C no miente. ■

Observación 3.3.12.— Desde un punto de vista sintáctico, lo que hemos demostrado es que $\rightarrow$ no se distribuye por la derecha en $\vee$. De hecho, de cómo se distribuye $\rightarrow$ en $\vee$, se satisfacen:

- la *distributiva por la izquierda*, $(p \rightarrow (q \vee r)) \leftrightarrow (p \rightarrow q) \vee (p \rightarrow r)$;
- la *semidistributiva por la derecha*, $((p \vee q) \rightarrow r) \rightarrow (p \rightarrow r) \vee (q \rightarrow r)$, y
- la *antidistributiva por la derecha*, $((p \vee q) \rightarrow r) \leftrightarrow (p \rightarrow r) \wedge (q \rightarrow r)$.

Ejemplo 161

«Dadas dos situaciones, del hecho de que ocurra alguna de ellas, siempre es posible inferir que ocurren ambas».

[Cubit 34], [AIC 10.4.2018:1B], [SEL 3:1].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si ocurre la situación P u ocurre la situación Q, entonces ocurre la situación P y ocurre la situación Q.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

   - *Variables proposicionales*.

     Siendo el universo de discurso el conjunto de todas las personas, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

     $$p \leftleftharpoons \text{Sucede la situación } P; \qquad q \leftleftharpoons \text{Sucede la situación } Q.$$

   - *Esquema argumental*:

     $$\begin{array}{rl} & \text{Se tiene } p \text{ o } q. \\ \hline \therefore & \text{Se sigue } p \text{ y } q. \end{array}$$

   - *Forma lógica*.

Identificamos el conjunto de premisas $\Phi = \{\phi_0\} = \{p \vee q\}$, con una única premisa, y la conclusión ψ, a saber, $p \wedge q$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $p \vee q \to p \wedge q$. Llamémosla A.

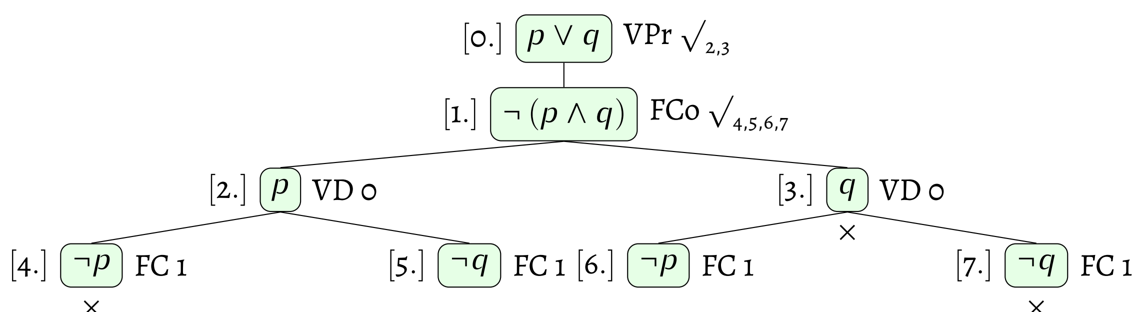
2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0\} \vDash \psi$. Refutar $\{\phi_0\} \vDash \psi$ es demostrar que $\phi_0 \wedge \neg\psi$ es una fórmula válida. Correspondiendo a dicha estructura, definimos $\Gamma = \{\phi_0\} \cup \{\neg\psi\} = \{p \vee q, \neg(p \wedge q)\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico.*

   Sea el árbol



   Observación.— VPr $\leftrightharpoons$ Verdad de la premisa; FCo $\leftrightharpoons$ Falsedad de la conclusión; FC $\leftrightharpoons$ Falsedad de la conjunción; VD $\leftrightharpoons$ Verdad de la disyunción.

   III. *Demostración de que es un árbol terminado.*

   Este árbol tiene un tronco, $\rho_0 = \langle p \vee q, \neg(p \wedge q)\rangle$, y cuatro ramas, a saber, $\rho_1 = \rho_0 +\!\!+ \langle p, \neg p\rangle$, $\rho_2 = \rho_0 +\!\!+ \langle p, \neg q\rangle$, $\rho_3 = \rho_0 +\!\!+ \langle q, \neg p\rangle$ y $\rho_4 = \rho_0 +\!\!+ \langle q, \neg q\rangle$.

   Es un árbol terminado, pues toda rama es insatisfactible o completa. En efecto:

   0. por un lado, ρ_1 y ρ_4 son ramas insatisfactibles, al existir en cada una de ellas una variable y su negación: p y $\neg p$ en ρ_1 y q y $\neg q$ en ρ_4;

   1. por otro, ρ_2 y ρ_3 son ramas satisfactibles y completas:

      0. en ρ_2 está $p \vee q$, estando también p y está $\neg(p \wedge q)$, estando también $\neg q$;

      1. en ρ_3 está $p \vee q$, estando también q y está $\neg(p \wedge q)$, estando también $\neg p$.

   IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existen dos ramas satisfactibles, ρ_2 y ρ_3, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), $p \wedge q$ no es consecuencia lógica de $\{p \vee q\}$, esto es, el argumento $\mathcal{A}$ no es válido e, igualmente, tampoco es válida la argumentación correspondiente.

3. *Identificación de los modelos para Γ que proporcionan las ramas satisfactibles.*

   Al ser ρ_2 y ρ_3 ramas satisfactibles, cada una de ellas proporciona un modelo para el conjunto de fórmulas bien formadas Γ, a saber:

   - ρ_2 proporciona el modelo $I(p) = 1$, $I(q) = 0$, abreviadamente, I_{10};
   - ρ_3 proporciona el modelo $I(p) = 0$, $I(q) = 1$, abreviadamente, I_{01}.

   En definitiva, las interpretaciones I_{10} e I_{01} son los únicos modelos para Γ.

4. *Demostración de que los modelos lo son para Γ.*

   No es difícil demostrar que I_{10} e I_{01} son modelos para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dichas interpretaciones:

p	q	p	$\vee$	q	$\neg$	$(p$	$\wedge$	$q)$
1	0	1	[1]	0	[1]	1	0	0
0	1	0	[1]	1	[1]	0	0	1

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

   Contraargumento: si ocurre sólo una de las situaciones, entonces ocurre una pero no ambas.

   Contraargumentación: no es válida la argumentación porque si sucede sólo una de las situaciones se satisface la premisa, ya que sucede alguna de las situaciones, pero precisamente por no suceder ambas situaciones, no se satisface la conclusión. ■

Ejemplo 162

«Lo digo yo sólo si lo dices tú. Así que, yo no lo digo pero tú sí».

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si yo lo digo, entonces tú lo dices. Luego, yo no lo digo y tú sí lo dices.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales.*

Siendo el universo de discurso el conjunto de todas las personas, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

$$p \leftrightharpoons \text{lo digo yo,}$$
$$q \leftrightharpoons \text{lo dices tú.}$$

- *Esquema argumental*:

  Si se supone p, se sigue q.

  ∴ Se sigue no p y q.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0\} = \{p \to q\}$, con una única premisa, y la conclusión ψ, a saber, $\neg p \wedge q$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $p \to q \to \neg p \wedge q$. Llamémosla A.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos*.

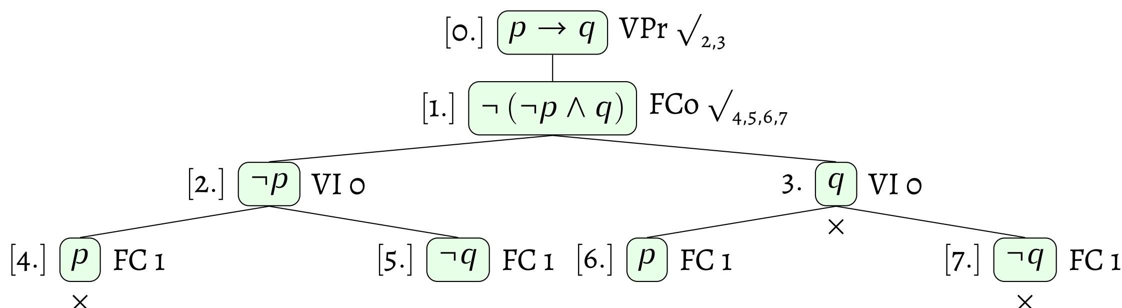
   I. *Identificación del conjunto* Γ.

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0\} \vDash \psi$. Refutar $\{\phi_0\} \vDash \psi$ es demostrar que $\phi_0 \wedge \neg\psi$ es una fórmula válida.

   Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0\} \cup \{\neg\psi\} = \{p \to q, \neg(\neg p \wedge q)\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico*.

   Sea el árbol



   Observación.— VPr $\leftrightharpoons$ Verdad de la premisa; FCo $\leftrightharpoons$ Falsedad de la conclusión; FC $\leftrightharpoons$ Falsedad de la conjunción; VI $\leftrightharpoons$ Verdad de la implicación.

   III. *Demostración de que es un árbol terminado*.

El tronco de este árbol es $\rho_0 = \langle p \rightarrow q, \neg(\neg p \land q)\rangle$ y sus cuatro ramas son $\rho_1 = \rho_0 \mathbin{+\!\!+} \langle \neg p, p\rangle$, $\rho_2 = \rho_0 \mathbin{+\!\!+} \langle \neg p, \neg q\rangle$, $\rho_3 = \rho_0 \mathbin{+\!\!+} \langle q, p\rangle$ y $\rho_4 = \rho_0 \mathbin{+\!\!+} \langle q, \neg q\rangle$.

Es un árbol terminado, pues toda rama es insatisfactible o completa. En efecto:

0. por un lado, ρ_1 y ρ_4 son ramas insatisfactibles, al existir en cada una de ellas una variable y su negación: p y $\neg p$ en ρ_1 y q y $\neg q$ en ρ_4;
1. por otro, ρ_2 y ρ_3 son ramas satisfactibles, pero completas: en ρ_2 está $p \rightarrow q$, estando también $\neg p$ y está $\neg(\neg p \land q)$, estando también $\neg q$; en ρ_3 está $p \rightarrow q$, estando también q y está $\neg(\neg p \land q)$, estando también $\neg\neg p$, esto es, p.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existen dos ramas satisfactibles, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), de $\{p \rightarrow q\}$, no se deduce $\neg p \land q$, esto es, el argumento $\mathcal{A}$ no es válido e, igualmente, tampoco es válida la argumentación correspondiente.

3. *Identificación de los modelos que proporcionan las ramas satisfactibles.*

Al ser ρ_2 y ρ_3 ramas satisfactibles, cada una de ellas proporciona un modelo para el conjunto de fórmulas bien formadas Γ, a saber,

- ρ_2 proporciona $I(p) = 0$ e $I(q) = 0$, abreviadamente, I_{00};
- ρ_3 proporciona $I(p) = 1$ e $I(q) = 1$, abreviadamente, I_{11}.

En definitiva, las interpretaciones I_{11} e I_{00} son los únicos modelos para Γ.

4. *Demostración de que los modelos lo son para Γ.*

No es difícil demostrar que I_{10} e I_{01} son modelos para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dichas interpretaciones:

p	q	p	$\rightarrow$	q	$\neg$	(	$\neg$	p	$\land$	q	)
1	1	1	[1]	1	[1]		0	1	0	1	
0	0	0	[1]	0	[1]		1	0	0	0	

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

- Contraargumentación proporcionada por el contramodelo I_{00}: Si yo no lo digo es verdadera la premisa, pues ésta consiste en la implicación que tiene por antecedente el yo decirlo; por otra parte, es falsa la conclusión, ya que ésta consiste en la conjunción de yo no decirlo y tú sí decirlo, pero el segundo conjunto es falso, ya que tú no lo dices.
- Contraargumentación proporcionada por el contramodelo I_{11}: Si yo lo digo y tú lo dices, es verdadera la premisa, pues ésta consiste en la implicación que tiene por antecedente el yo

decirlo y por consecuente el tú decirlo; por otra parte, es falsa la conclusión, ya que ésta consiste en la conjunción de yo no decirlo y tú sí decirlo, pero el primer conjunto es falso, ya que yo sí lo digo. ■

Ejemplo 163

«Que vayamos a la vez es un absurdo, por tanto no vas tú o voy yo».

[Cubit 38], [SEL 3:6].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si tú vas y yo voy, entonces se tiene una contradicción. Luego, si tú vas, entonces yo voy.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales.*

     Siendo el universo de discurso el conjunto de todas las personas, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

     $$p \risingdotseq \text{vas tú}; \qquad q \risingdotseq \text{voy yo}.$$

   - *Esquema argumental*:

	Si se supone p y q, se sigue una contradicción.
$\therefore$	Se sigue que si se supone p, se sigue q.

   - *Forma lógica.*

     Identificamos el conjunto de premisas $\Phi = \{\phi_0\} = \{p \wedge q \to \bot\}$, con una única premisa, y la conclusión ψ, a saber, $p \to q$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(p \wedge q \to \bot) \to (p \to q)$. Llamémosla A.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

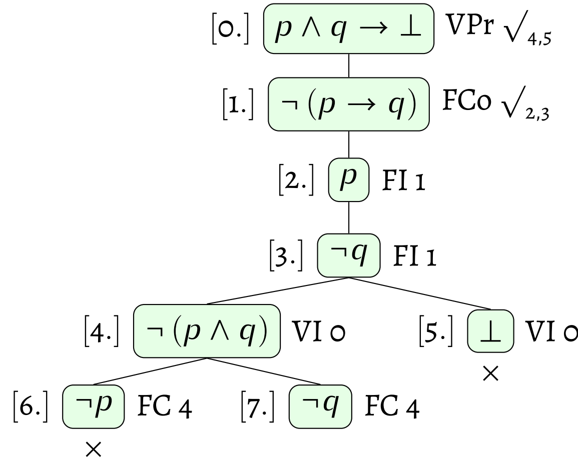
   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0\} \vDash \psi$. Refutar $\{\phi_0\} \vDash \psi$ es demostrar que $\phi_0 \wedge \neg\psi$ es una fórmula válida.

   Correspondiendo a dicha estructura, definimos $\Gamma = \{\phi_0\} \cup \{\neg\psi\} = \{p \wedge q \to \bot, \neg(p \to q)\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

II. *Construcción anotada del árbol semántico.*

Sea el árbol:



Observación.—VPr ⥱ Verdad de la premisa; FCo ⥱ Falsedad de la conclusión; FC ⥱ Falsedad de la conjunción; FI ⥱ Falsedad de la implicación; VI ⥱ Verdad de la implicación.

III. *Demostración de que es un árbol terminado.*

Este árbol tiene un tronco, $\rho_0 = \langle p \wedge q \rightarrow \bot, \neg(p \rightarrow q)\rangle$ y tres ramas: $\rho_1 = \rho_0 \mathbin{+\!\!+} \langle p, \neg q, \neg(p \wedge q), \neg p\rangle$; $\rho_2 = \rho_0 \mathbin{+\!\!+} \langle p, \neg q, \neg(p \wedge q), \neg q\rangle$, y $\rho_3 = \rho_0 \mathbin{+\!\!+} \langle p, \neg q, \bot\rangle$.

Es un árbol terminado, pues toda rama es insatisfactible o completa. En efecto:

0. por un lado, ρ_1 y ρ_3 son ramas insatisfactibles, pues ρ_1 incluye una variable y su negación: p y $\neg p$ y ρ_3 incluye a la contradicción $\bot$;

1. por otro, ρ_2 es una rama satisfactible, aunque completa: en ρ_2 está $p \wedge q \rightarrow \bot$, estando también $\neg(p \wedge q)$, está $\neg(p \rightarrow q)$, estando también p y $\neg q$ y está $\neg(p \wedge q)$, estando también $\neg p$.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existen ramas satisfactibles, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), de $p \wedge q \rightarrow \bot$, no se deduce $p \rightarrow q$, esto es, el argumento $\mathcal{A}$ no es válido e, igualmente, tampoco es válida la argumentación correspondiente.

3. *Identificación de los modelos para Γ que proporcionan las ramas satisfactibles.*

Al ser ρ_2 satisfactible, proporciona un modelo para Γ, concretamente, $I(p) = 1$, $I(q) = 0$, abreviadamente, I_{10}.

4. *Demostración de que los modelos lo son para Γ.*

No es difícil demostrar que I_{10} es un modelo para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dicha interpretación:

p q	(p ∧ q) → ⊥	¬ (p → q)
1 0	1 0 0 [1] 0	[1] 1 0 0

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

Hemos hallado una refutación para la afirmación propuesta, puesto que si sucede que si vas tú pero no voy yo, no se satisface dicha afirmación. En efecto:

- Contraargumentación proporcionada por I_{10}: Si tú vas y yo no voy, es verdadera la premisa, pues ésta es la implicación que tiene por antecedente la conjunción de ir tú y yo, y ser ésta falsa por no ir yo; por otra parte, es falsa la conclusión, ya que ésta consiste en la implicación de antecedente ir tú (verdadero) y consecuente ir yo (falso). ■

Observación 3.3.13.— En vez de por $p \wedge q \rightarrow \perp$ [ir a la vez es lo que da lugar al absurdo; si no vamos a la vez, ¿quién sabe?], pudiésemos haber representado la premisa en lógica de juntores por $\neg(p \wedge q)$, fórmula lógicamente equivalente a la anterior.

Con el ánimo de reflejar cómo aparecen las TA/S en otros textos, vemos en los siguientes dos ejemplos una variante de su representación. Ésta es, por ejemplo, la utilizada por Hodges [92]. Por otro lado, la observación 3.3.14 (pág. 318 de esta edición) muestra una representación algo anterior en el tiempo, que quizás ilustre nuestro entendimiento del porqué del nombre de tabla.

Ejemplo 164

> «Sabemos que Cala viene siempre que viene Abigail. También sabemos que Cala viene si viene Balbina. Y nos han dicho que es seguro que una de las dos, Abigail o Balbina, va a venir. Así que también es seguro que Cala vendrá».
>
> ---
> [EFE 29.6.2018:1b2].

Resolución.— En el ejemplo 137 (pág. 230 de esta edición) resolvimos esta argumentación por reducción al absurdo (Abs, RAA).

0. y 1. En dicho ejemplo resolvimos los apartados 0 y 1 que aquí se piden, esto es, allí: 0.º, hallamos el argumento $\mathcal{A}$ correspondiente; 1.º, propusimos su formalización (variables proposicionales, esquema argumental y forma lógica) en lógica de juntores; 2.º, identificamos el conjunto de premi-

sas $\Phi = \{\phi_0, \phi_1, \phi_2\} = \{A \to C, B \to C, A \lor B\}$ y la conclusión ψ, a saber, C, y 3.º, sugerimos la forma lógica en lógica de juntores para $\mathcal{A}$, que resultó ser $(A \to C) \land (B \to C) \land (A \lor B) \to C$.

Ahora queremos resolver $\mathcal{A}$ mediante TA/S, utilizando ésta para dilucidar si C es consecuencia lógica de $\{A \to C, B \to C, A \lor B\}$, esto es, si $\{A \to C, B \to C, A \lor B\} \vDash C$.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

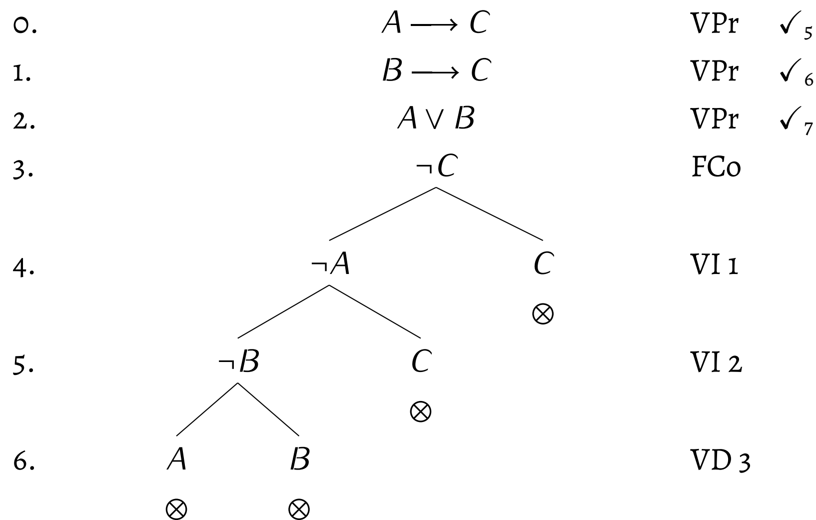
   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1, \phi_2\} \vDash \psi$. Refutar $\{\phi_0, \phi_1, \phi_2\} \vDash \psi$ es demostrar que $\phi_0 \land \phi_1 \land \phi_2 \land \neg\psi$ es una fórmula válida.

   Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0, \phi_1, \phi_2\} \cup \{\neg\psi\} = \{A \to C, B \to C, A \lor B, \neg C\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico.*

   Sea el árbol:



   Observación.—VPr $\leftrightharpoons$ Verdad de la premisa; FCo $\leftrightharpoons$ Falsedad de la conclusión; VI $\leftrightharpoons$ Verdad de la implicación; VD $\leftrightharpoons$ Verdad de la disyunción.

   III. *Demostración de que es un árbol terminado.*

   El tronco (conjunto de nodos iniciales comunes) ρ_0 de este árbol es $\rho_0 = \langle A \to C, B \to C, A \lor B, \neg C\rangle$ y sus cuatro ramas son:

$\rho_1 = \rho_0 \mathbin{+\!\!+} \langle \neg A, \neg B, A\rangle$, $\rho_3 = \rho_0 \mathbin{+\!\!+} \langle \neg A, C\rangle$,
$\rho_2 = \rho_0 \mathbin{+\!\!+} \langle \neg A, \neg B, B\rangle$, $\rho_4 = \rho_0 \mathbin{+\!\!+} \langle C\rangle$.

Es un árbol terminado, pues toda rama es insatisfactible al existir en cada una de ellas al menos una variable y su negación: A y $\neg A$ en ρ_1; B y $\neg B$ en ρ_2, y C y $\neg C$ en ρ_3 y ρ_4.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como todas las ramas son insatisfactibles, este árbol terminado es insatisfactible, por lo que hemos demostrado que Γ es un conjunto insatisfactible de fórmulas, en otras palabras, hemos encontrado una refutación para Γ, esto es, para $\{\phi_0, \phi_1, \phi_2\} \cup \{\neg\psi\}$, lo cual, por el teorema 3.8 (pág. 281 de esta edición), sabemos que es equivalente a que $\{\phi_0, \phi_1, \phi_2\} \vDash \psi$, es decir, a que $\phi_0 \wedge \phi_1 \wedge \phi_2 \rightarrow \psi$ sea una fórmula válida, en otras palabras, a que $\mathcal{A}$ sea válido el argumento $\mathcal{A}$ e, igualmente, sea válida la argumentación correspondiente.

3. No procede (no hay ramas satisfactibles).

4. No procede (no hay modelos para Γ).

5. No procede (no hay contraargumentaciones). ■

Ejemplo 165

Una aplicación contiene dos tipos de componentes software, las correctas (se sabe que están libres de errores) y las incorrectas (se sabe que no están libres de errores). Toda componente de la aplicación es de alguno de los dos tipos. La aplicación ha fallado. El análisis de la situación arroja lo siguiente: 0.º, sólo se sospecha de tres componentes, A, B y C y se sabe que al menos una es incorrecta; 1.º, de ser A incorrecta, nunca podría fallar en solitario, fallaría junto al menos a otra componente, y 2.º, C es una componente correcta. Con estos datos, el personal investigador concluyó que B y C eran componentes correctas.

[Cubit 39], [EFE 7.7.2017:9], [SEL 3:10]. *Cfr.* Manzano y Huertas [62] 4.5 Mafia, Mafia(2) Robo de archivos (pág. 101).

Resolución.—

0. *Argumento* ($\mathcal{A}$): A es una componente incorrecta o B es una componente incorrecta o C es una componente incorrecta. Si A es una componente incorrecta, entonces B es una componente incorrecta o C es una componente incorrecta. C no es una componente incorrecta. Luego, B no es una componente incorrecta y C no es una componente incorrecta.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales*:

Siendo el universo de discurso el conjunto de todas las componentes software, sean tres las variables proposicionales y las proposiciones simples que representan:

$$A \risingdotseq A \text{ es una componente incorrecta;}$$
$$B \risingdotseq B \text{ es una componente incorrecta;}$$
$$C \risingdotseq C \text{ es una componente incorrecta.}$$

- *Esquema argumental*:

  Se tiene A o B o C.
  Si se supone A, se sigue B o C.
  Se tiene no C.

  $\therefore$ Se sigue no B y no C.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2\} = \{(A \vee B) \vee C, A \rightarrow (B \vee C), \neg C\}$ y la conclusión ψ, a saber, $\neg B \wedge \neg C$.

  La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(A \vee B \vee C) \wedge (A \rightarrow (B \vee C)) \wedge \neg C \rightarrow \neg B \wedge \neg C$. Llamémosla A.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos*.

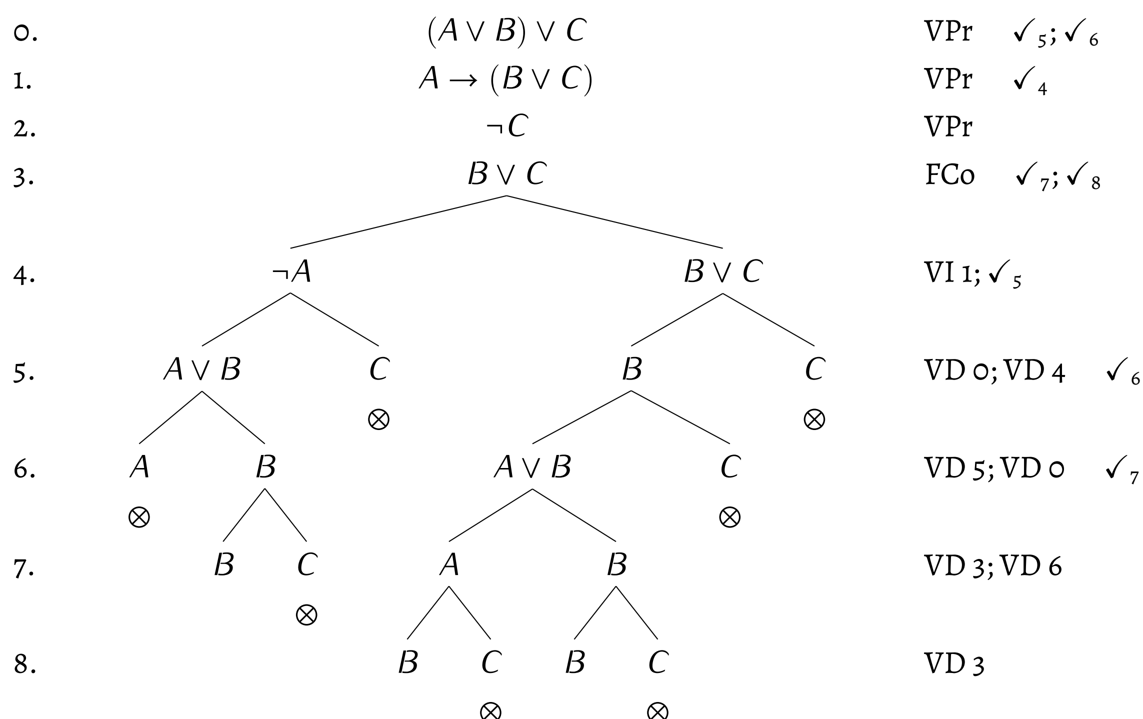
   I. *Identificación del conjunto* Γ.

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1, \phi_2, \phi_3\} \vDash \psi$. Refutar $\{\phi_0, \phi_1, \phi_2, \phi_3\} \vDash \psi$ es demostrar que $\phi_0 \wedge \phi_1 \wedge \phi_2 \wedge \phi_3 \wedge \neg\psi$ es una fórmula válida.

   Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0, \phi_1, \phi_2, \phi_3\} \cup \{\neg\psi\} = \{(A \vee B) \vee C, A \rightarrow (B \vee C), \neg C, B \vee C\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico*.

   El árbol semántico es



Observación.— El punto y coma separa lo aplicado en los dos subárboles de raíces respectivas $\neg A$ y $B \vee C$. Los acrónimos utilizados son: VPr ⥋ Verdad de la premisa; FCo ⥋ Falsedad de la conclusión; VI ⥋ Verdad de la implicación; VD ⥋ Verdad de la disyunción.

III. *Demostración de que es un árbol terminado.*

Este árbol tiene un tronco ρ_0 (el conjunto de nodos iniciales comunes),

$$\rho_0 = \langle (A \vee B) \vee C, A \to (B \vee C), \neg C, B \vee C \rangle,$$

y diez ramas:

$\rho_1 = \rho_0 +\!\!+ \langle \neg A, A \vee B, A \rangle,$
$\rho_2 = \rho_0 +\!\!+ \langle \neg A, A \vee B, B, B \rangle,$
$\rho_3 = \rho_0 +\!\!+ \langle \neg A, A \vee B, B, C \rangle,$
$\rho_4 = \rho_0 +\!\!+ \langle \neg A, C \rangle,$
$\rho_5 = \rho_0 +\!\!+ \langle B \vee C, B, A \vee B, A, B \rangle,$
$\rho_6 = \rho_0 +\!\!+ \langle B \vee C, B, A \vee B, A, C \rangle,$
$\rho_7 = \rho_0 +\!\!+ \langle B \vee C, B, A \vee B, B, B \rangle,$
$\rho_8 = \rho_0 +\!\!+ \langle B \vee C, B, A \vee B, B, C \rangle,$
$\rho_9 = \rho_0 +\!\!+ \langle B \vee C, B, C \rangle,$
$\rho_{10} = \rho_0 +\!\!+ \langle B \vee C, C \rangle.$

Es un árbol terminado, pues, por un lado, las ramas ρ_1, ρ_3, ρ_4, ρ_6, ρ_8, ρ_9 y ρ_{10}, son insatisfactibles al existir en cada una de ellas al menos una variable y su negación:

- A y $\neg A$ en ρ_1, y
- C y $\neg C$ en ρ_3, ρ_4, ρ_6, ρ_8, ρ_9 y ρ_{10}.

Por otro, las ramas ρ_2, ρ_5 y ρ_7 son satisfactibles pero completas; en efecto,

- ρ_2 es completa porque: respecto de $(A \vee B) \vee C$, el disyunto $A \vee B$ es un elemento de ρ_2; respecto de $A \to (B \vee C)$, el disyunto $\neg A$ es un elemento de ρ_2, y respecto de $B \vee C$, el disyunto B es un elemento de ρ_2;
- ρ_5 es completa porque: respecto de $(A \vee B) \vee C$, el disyunto $A \vee B$ es un elemento de ρ_5; respecto de $A \to (B \vee C)$, el disyunto $B \vee C$ es un elemento de ρ_5, y respecto de $B \vee C$, el disyunto B es un elemento de ρ_5;
- ρ_7 es completa porque: respecto de $(A \vee B) \vee C$, el disyunto $A \vee B$ es un elemento de ρ_7; respecto de $A \to (B \vee C)$, el disyunto $B \vee C$ es un elemento de ρ_7, y respecto de $B \vee C$, el disyunto B es un elemento de ρ_7.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existen ramas satisfactibles, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), de $(A \vee B \vee C) \wedge (A \to (B \vee C)) \wedge \neg C$, no se deduce $\neg B \wedge \neg C$, esto es, el argumento $\mathcal{A}$ no es válido e, igualmente, tampoco es válida la argumentación correspondiente.

3. *Identificación de los modelos que proporcionan las ramas satisfactibles.*

Los modelos proporcionados por las ramas satisfactibles son los siguientes:

- ρ_2 proporciona el modelo 010, esto es $I_{010}(A) = 0$, $I_{010}(B) = 1$, $I_{010}(C) = 0$;
- ρ_5 proporciona el modelo 110, esto es $I_{110}(A) = 1$, $I_{110}(B) = 1$, $I_{110}(C) = 0$;
- ρ_7 proporciona los dos modelos anteriores.

En definitiva, las interpretaciones I_{010} e I_{110} son los únicos modelos para Γ.

4. *Demostración de que los modelos lo son para Γ.*

No es difícil demostrar que I_{010} e I_{110} son modelos para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dichas interpretaciones:

A	B	C	(A	∨	B)	∨	C	A	→	(B	∨	C)	¬	C	B	∨	C
1	1	0	1	1	1	[1]	0	1	[1]	1	1	0	[1]	0	1	[1]	0
0	1	0	0	1	1	[1]	0	0	[1]	1	1	0	[1]	0	1	[1]	0

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

Contraargumentación constuida a partir de I_{110}: Si A y B son componentes incorrectas y C no lo es, se satisface: por un lado, la disyunción de ser incorrectas las tres, por ser incorrectas A y B; por otro, la disyunción de ser B incorrecta y C no serlo —por satisfacerse ambos disyuntos— y, por lo tanto, la implicación que tiene a esta disyunción de consecuente a ser A incorrecta de

antecedente; por otro, C no es incorrecta, y, sin embargo, la conclusión no es cierta, pues la conjunción de no ser B ni C componentes incorrectas no lo es al ser B una componente incorrecta.

Contraargumentación constuida a partir de I_{010}: Si A y C no son componentes incorrectas y B sí lo es, se satisface: por un lado, la disyunción de ser incorrectas las tres, por ser incorrecta B; por otro, la implicación que tiene de antecedente ser A incorrecta es verdadera precisamente por no serlo A y ser falso dicho antecendente; por otro, C no es incorrecta, y, sin embargo, la conclusión no es cierta, pues la conjunción de no ser B ni C componentes incorrectas no lo es al ser B una componente incorrecta. ■

Observación 3.3.14.— Las primeras representaciones de TA/S eran del estilo de la siguiente (equivalentes, en cualquier caso, al árbol semántico estudiado).

(0) $(A \vee B) \vee C$ VPr $\checkmark_{8,9}$ $\checkmark_{10,11}$
(1) $A \rightarrow (B \vee C)$ VPr $\checkmark_{4,5}$
(2) $\neg C$ VPr
(3) $B \vee C$ FCo $\checkmark_{16,17}$ $\checkmark_{18,19}$ $\checkmark_{20,21}$
(4) $\neg A$ [VI 2] | (5) $B \vee C$ [VI 2] $\checkmark_{6,7}$
(8) $A \vee B$ [VD 1] $\checkmark_{12,13}$ | (9) $\underset{\times}{C}$ [VD 1] | (6) B [VD 5] | (7) $\underset{\times}{C}$ [VD 5]
(12) $\underset{\times}{A}$ [VD 8] | (13) B [VD 8] | (10) $A \vee B$ [VD 1] $\checkmark_{14,15}$ | (11) $\underset{\times}{C}$ [VD 1]
(16) B [VD 3] | (17) $\underset{\times}{C}$ [VD 3] | (14) A [VD 10] | (15) B [VD 10]
(18) B [VD 3] | (19) $\underset{\times}{C}$ [VD 3] | (20) B [VD 3] | (21) $\underset{\times}{C}$ [VD 3]

Observación.— VPr $\leftrightharpoons$ Verdad de la premisa; FCo $\leftrightharpoons$ Falsedad de la conclusión; VD $\leftrightharpoons$ Verdad de la disyunción; VI $\leftrightharpoons$ Verdad de la implicación.

Observación 3.3.15.— Si hubiésemos formalizado $X \leftrightharpoons X$ es una componente correcta, entonces la formalización del argumento hubiese sido $(\neg A \vee \neg B) \vee \neg C, \neg A \rightarrow (\neg B \vee \neg C), C \vdash B \wedge C$.

Observación 3.3.16.— Por hacer un símil en paralelo, las componentes correctas serían como las personas veraces (nunca fallan/mienten), las incorrectas como las personas normales (a veces fallan/mienten, a veces no) y las componentes fastidiadas como las personas falaces (siempre fallan/mienten).

§ 3.3.8 TA/S y RAA

Una vez que ya hemos tenido oportunidad de estudiar y reflexionar sobre el método de las tablas analíticas/semánticas (TA/S), es el momento de ampliar la observación 3.3.4 (pág. 281 de esta edición).

El hecho es que pudiésemos interpretar TA/S como una reducción al absurdo (Abs, RAA). En efecto, en la resolución de una cuestión vía TA/S, tanto si se trata de demostrar que $\vDash \phi$ o que $\Phi \vDash \psi$ —esto es, que $\vdash \phi$ o que $\Phi \vdash \psi$, en el ámbito sintáctico—, partimos de negar la fórmula en lógica de juntores que representa la situación y,

- si esto nos lleva a un árbol insatisfactible, esto es, un árbol en el que todas sus ramas (conjuntos de fórmulas) son insatisfactibles, es decir, un árbol en el que para cualquiera de sus ramas no existe ningún modelo —en términos sintácticos, un árbol en el que en todas sus ramas hemos localizado una contradicción—, entonces TA/S nos asegura que la fórmula es válida; resumiendo, y en analogía con la reducción al absurdo, si suponer la negación de la fórmula nos lleva a una contradicción (ya que, y esta es la clave, todos los caminos posibles de deducción —ramas— nos conducen a una contradicción), deducimos que la fórmula es válida [este hecho se corresponde, ya en lógica de juntores, con $(\neg\phi \to \bot) \to \phi$];
- mientras que si alguna de las ramas resulta ser satisfactible —esto es, en términos sintácticos, si no localizamos una contradicción en alguna rama—, entonces, en analogía con la reducción al absurdo, suponer la negación de la fórmula no nos lleva a una contradicción (pues hay algún camino posible de deducción que no nos lleva a contradicción), por lo que deducimos que la fórmula es no válida (pudiendo ser contingente o insatisfactible) [este hecho se corresponde, ya en lógica de juntores, con $\neg(\neg\phi \to \bot) \to \neg\phi$].

§ 3.3.9 Algunos artefactos software

Existen artefactos en línea de utilización gratuita para hallar el árbol semántico —algunas personas seguro que utilizaremos algunos de ellos en nuestra práctica profesional—.

Algunos de ellos son los siguientes. Como muestra, veamos la aplicación de los cuatro que destacamos a dos ejemplos de deducciones semánticas:

I. $\{(p \wedge q) \to r\} \vDash p \to (q \to r)$ (ley de exportación);

II. $\{A \to C, B \to C, A \vee B\} \vDash C$.

- En línea.
  0. The Truth Tree Solver[32], que resuelve las deducciones anteriores, por ejemplo con las siguientes entradas respectivas:
     I. `((P and Q) then R) and not (P then (Q then R))`;
     II. `(A then C) and (((B then C) and (A or B)) and not C)`;
  1. logic-rs[33], que resuelve las deducciones anteriores, por ejemplo con las siguientes entradas respectivas:
     I. `(P & Q) ⊃ R` (en la línea 1), `∴ P ⊃ (Q ⊃ R)` (en la línea 2);

[32] The Truth Tree Solver (http://www.formallogic.com/en/truth-tree-solver) (©gratisOA), de Gabriel Lemonde-Labrecque (https://github.com/gablem).
[33] logic-rs (https://ixjf.github.io/logic-rs/) (©gratisOA), de Pedro Fanha, alias ixjf (https://github.com/ixjf).

II. `(A ⊃ C),` (en la línea 1), `(B ⊃ C),` (en la línea 2), `(A ∨ B)` (en la línea 3) y `∴ C` (en la línea 4);

2. pytableaux[34], que resuelve las deducciones anteriores, eligiendo CPL (*Classical Predicate Logic*), por ejemplo con las siguientes entradas respectivas:

   I. `(A & B ) > C` (en P1) y `A > (B > C)` (en C);

   II. `A > C` (en P1), `B > C` (en P2), `A V C` (en P3) y `C` (en C);

3. Tree Proof Generator[35], que resuelve las deducciones anteriores, por ejemplo con las siguientes entradas respectivas:

   I. `(p and q) then r |= p then (q then r)`;

   II. `(A then C) and (B then C) and (A or B) |= C`.

4. Logic Calculator[36].

5. My Logic Hub[37].

- De escritorio.

6. ProofTools[38].

Laird SHAW[39], el programador de ProofTools, mantiene una comparativa de algunos artefactos[40].

Por otra parte, pudiésemos haber escrito un programa en algún lenguaje de programación conveniente o favorito, por ejemplo, logic-rs[33] o *Semantic Tableaux in Less than 90 Lines of Scala*[41].

---

[34] pytableaux (https://logic.dougowings.net/) (©GNU Affero General Public License), de Doug OWINS; este artefacto en línea permite además el estudio de creación nodo a nodo del árbol, con notificación de la regla utilizada en cada paso.

[35] Tree Proof Generator (https://www.umsu.de/trees/) (©gratisOA), de Wolfgang SCHWARZ (https://www.umsu.de/), sólo para árboles insatisfactibles (para los satisfactibles proporciona un contramodelo) (antes, estaba funcional el artefacto en línea https://www.umsu.de/logik/oldtrees/ que construía ambos tipos de tablas semánticas, insatisfactibles y satisfactibles).

[36] Logic Calculator —de Christian GOTTSCHALL (https://www.erpelstolz.at/christian/homepage-uk.html), en Gateway to Logic (https://www.erpelstolz.at/gateway/)—, en su versión del lado del servidor, debemos elegir en el desplegable «Task to be performed» [Tarea para ser realizada], «Prove the proposition» [Demostrar la proposición], cuya sintaxis específica podemos consultar en https://www.erpelstolz.at/gateway//prover.html (si bien probablemente sea una buena idea volver a leer lo escrito sobre Logic Calculator en la observación 1.8.1 (pág. 134 de esta edición) para recordar la sintaxis ya aprendida en su uso como generador de tablas de verdad).

[37] My Logic Hub (https://www.mylogichub.com) (©GNU General Public License v3), de Fouzan TARIQ (https://github.com/kror-shack/my-logic-hub).

[38] ProofTools (https://creativeandcritical.net/prooftools) (©GNU Affero General Public License), de Laird SHAW (https://creativeandcritical.net/about-laird-shaw) —y Emil KIRKEGAARD (http://emilkirkegaard.dk/)—.

[39] Acerca de Laird SHAW: https://creativeandcritical.net/about-laird-shaw.

[40] *A feature comparison of free proof tree aka semantic tableau software* (https://creativeandcritical.net/prooftools/comparison-of-proof-tree-semantic-tableau-software) (©Dominio Público Anticipado).

[41] *Semantic Tableaux in Less than 90 Lines of Scala* (http://voidmainargs.blogspot.com/2011/09/semantic-tableaux-in-less-than-90-lines.html) (©gratisOA), de voidmainargs (https://www.blogger.com/profile/00911109433888554531), en void-main-args (http://voidmainargs.blogspot.com/).

§ 3.3.10 Muestra de más ejemplos de TA/S

Los siguientes cuatro son ejemplos de utilización de los cuatro primeros artefactos en línea anteriores, The Truth Tree Solver, logic-rs, pytableaux y Tree Proof Generator, con motivo de que nos acostumbremos a las diferentes representaciones del árbol semántico que nos ofrecen. Quien lee es libre de utilizar Logic Calculator, también en línea, o ProofTools, de escritorio.

Ejemplo 166

«Ningún equipo que participa es capaz nunca de entrenar durante tres meses. Ningún equipo que participa está seguro de estar bien preparado a menos que sea capaz de entrenar durante tres meses. Por tanto, si es un equipo que participa, entonces ni está seguro de su buena preparación ni es capaz de entrenar durante tres meses».

[EFO 17.1.2022:1], [PEP 5.4.2022:1].

Resolución.—

0. *Argumento*.

- *Reescritura de la argumentación*.

  Detengámonos un momento en la segunda oración. La declaración «No sucede X a menos que suceda Y» expresa la necesidad de que suceda Y para que suceda X, es decir, «Que suceda Y es condición necesaria para que suceda X», en otras palabras, «Si X, entonces Y».

  Reescribimos la segunda oración en la forma «No sucede X a menos que suceda Y», esto es, así: «No puede tratarse de un equipo que participa y está seguro de su buena preparación, a menos que se trate de un equipo capaz de entrenar durante tres meses».

  Por lo comentado, volvemos a reescribirla, ahora en la forma «Si X, entonces Y», es decir, así: «Si se trata de un equipo que participa y está seguro de su buena preparación, entonces se trata de un equipo capaz de entrenar durante tres meses».

- *Argumento* ($\mathcal{A}$): Si se trata de un equipo que participa, entonces no se trata de un equipo capaz de entrenar durante tres meses. Si se trata de un equipo que participa y está seguro de su buena preparación, entonces se trata de un equipo capaz de entrenar durante tres meses. Por tanto, si se trata de un equipo que participa, entonces ni se trata de un equipo

seguro de su buena preparación ni se trata de un equipo capaz de entrenar durante tres meses.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales.*

     Siendo el universo de discurso el conjunto de todas las personas, consideramos las siguientes funciones proposicionales y sus descripciones:

     $P(s) \fallingdotseq$ s es un equipo que participa;

     $Q(s) \fallingdotseq$ s es un equipo seguro de su buena preparación;

     $R(s) \fallingdotseq$ s es un equipo capaz de entrenar durante tres meses.

     Como es habitual, para facilitar el cálculo lógico, sustituimos las funciones proposicionales $P(s)$, $Q(s)$ y $R(s)$ por una sola letra p, q y r, respectivamente.

   - *Esquema argumental*:

     Si se supone p, se sigue $\neg r$.
     Si se supone $p \wedge q$, se sigue r.

     $\therefore$ Se sigue que si se supone p, se sigue $\neg q \wedge \neg r$.

   - *Forma lógica.*

     Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{p \rightarrow \neg r, (p \wedge q) \rightarrow r\}$, con una única premisa, y la conclusión ψ, a saber, $p \rightarrow (\neg q \wedge \neg r)$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(p \rightarrow \neg r) \wedge ((p \wedge q) \rightarrow r) \rightarrow (p \rightarrow (\neg q \wedge \neg r))$. Llamémosla A.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

   1. *Identificación del conjunto Γ.*

      De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con ser $(p \rightarrow \neg r) \wedge ((p \wedge q) \rightarrow r) \rightarrow (p \rightarrow (\neg q \wedge \neg r))$ una fórmula válida, esto es, con $\vDash (p \rightarrow \neg r) \wedge ((p \wedge q) \rightarrow r) \rightarrow (p \rightarrow (\neg q \wedge \neg r))$. Refutar $\vDash \phi_0 \wedge \phi_1 \rightarrow \psi$ es demostrar que $\phi_0 \wedge \phi_1 \wedge \neg \psi$ es una fórmula válida.

      Correspondiendo a dicha estructura deductiva, definimos

$$\begin{aligned}\Gamma &= \{\neg(\phi_0 \wedge \phi_1 \rightarrow \psi)\}\\ &= \{\neg((p \rightarrow \neg r) \wedge ((p \wedge q) \rightarrow r) \rightarrow (p \rightarrow (\neg q \wedge \neg r)))\}\\ &= \{(p \rightarrow \neg r) \wedge ((p \wedge q) \rightarrow r) \wedge \neg(p \rightarrow (\neg q \wedge \neg r))\}\,.\end{aligned}$$

Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

II. *Construcción anotada del árbol semántico.*

Vemos el árbol generado por *Truth Tree Solver* en la figura 3.0 (pág. 323 de esta edición).

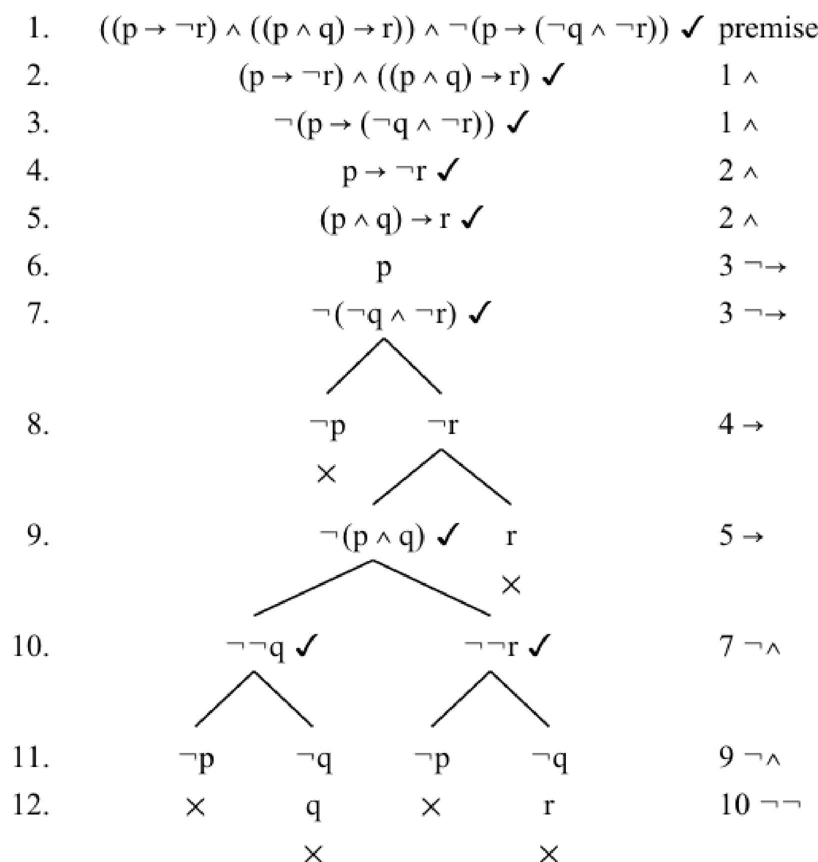


Figura 3.0.—Árbol semántico correspondiente a Γ que genera el artefacto en línea *Truth Tree Solver* con la entrada `((p then not r) and ((p and q) then r)) and not (p then (not q and not r))`. La notación es la de Barker-Plummer, Barwise, Etchemendy, Liu, Murray y Pease [93].

Actividad 3.3

Como vemos, este artefacto en línea utiliza otra notación para anotar el árbol; por un lado, entendámosla, por otro, anotémoslo convenientemente utilizando nuestra notación habitual.

III. *Demostración de que es un árbol terminado.*

Este árbol tiene el tronco ρ_0 de nodos iniciales comunes,

$$\rho_0 = \langle (p \to \neg r) \wedge ((p \wedge q) \to r) \wedge \neg(p \to (\neg q \wedge \neg r)), (p \to \neg r) \wedge ((p \wedge q) \to r), \neg(p \to (\neg q \wedge \neg r)), p \to \neg r, (p \wedge q) \to r, p, \neg(\neg q \wedge \neg r) \rangle,$$

y las seis ramas:

$\rho_1 = \rho_0 \mathbin{+\!\!+} \langle \neg p \rangle$, $\rho_4 = \rho_0 \mathbin{+\!\!+} \langle \neg r, \neg(p \wedge q), \neg\neg r, \neg p \rangle$,
$\rho_2 = \rho_0 \mathbin{+\!\!+} \langle \neg r, \neg(p \wedge q), \neg\neg q, \neg p \rangle$, $\rho_5 = \rho_0 \mathbin{+\!\!+} \langle \neg r, \neg(p \wedge q), \neg\neg r, \neg q, r \rangle$,
$\rho_3 = \rho_0 \mathbin{+\!\!+} \langle \neg r, \neg(p \wedge q), \neg\neg q, \neg q, q \rangle$, $\rho_6 = \rho_0 \mathbin{+\!\!+} \langle \neg r, r \rangle$.

Es un árbol terminado, pues toda rama es insatisfactible al existir en cada una de ellas al menos una variable y su negación: p y $\neg p$ en ρ_1, ρ_2 y ρ_4; q y $\neg q$ en ρ_3, y r y $\neg r$ en ρ_5 y ρ_6.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como todas las ramas son insatisfactibles, este árbol terminado es insatisfactible, por lo que hemos demostrado que Γ es un conjunto insatisfactible de fórmulas, en otras palabras, hemos demostrado que existe una refutación para Γ (traducido a $\mathcal{L}_0$, para $\phi_0 \wedge \phi_1 \wedge \neg\psi$), lo cual, por el teorema 3.8 (pág. 281 de esta edición), equivale a haber demostrado $\vDash \phi_0 \wedge \phi_1 \to \psi$, es decir, a que $\phi_0 \wedge \phi_1 \to \psi$ sea una fórmula válida, en otras palabras, a que $\mathcal{A}$ sea válido el argumento $\mathcal{A}$ e, igualmente, sea válida la argumentación correspondiente.

3. No procede (no hay ramas satisfactibles).

4. No procede (no hay modelos para Γ).

5. No procede (no hay contraargumentaciones). ■

Observación 3.3.17.— Cualquier proposición admite una pluralidad de expresiones lógicamente equivalentes. Está en su naturaleza, una proposición es una clase de equivalencia de oraciones declarativas. Por ejemplo, insistiendo en la segunda premisa, pudiésemos reescribirla también en la forma «Si se trata de un equipo que participa y no se trata de un equipo capaz de entrenar durante tres meses, entonces no se trata de un equipo seguro de su buena preparación», que con esta formalización es «Si se supone $p \wedge \neg r$, se sigue $\neg q$» —seguramente menos sencilla de entender, aunque para convencernos, pudiésemos, por ejemplo, demostrar mediante una tabla de verdad que $(p \wedge q) \to r$ es lógicamente equivalente a $(p \wedge \neg r) \to \neg q$—. Igualmente pudiésemos pensar en expresiones lógicamente equivalentes de las otras oraciones, por ejemplo, algunas de la primera premisa: $p \to \neg r \Leftrightarrow \neg p \vee \neg q \Leftrightarrow \neg(p \wedge r) \Leftrightarrow (p \wedge \neg r) \vee \neg p$.

Observación 3.3.18.— A veces, es posible construir un razonamiento completo en breves líneas a partir del esquema argumental; por ejemplo, en el caso que nos ocupa:

0.º, si se supone p, entonces se sigue $\neg r$ [1.ª premisa] $(*)$;

1.º, de $\neg r$ se sigue $\neg(p \wedge q)$, esto es, $\neg p \vee \neg q$ (†) [2.ª premisa, contrapositiva y ley de DE MORGAN],

2.º, de donde, como se supone p, no se sigue $\neg p$, por lo que de (†) se sigue $\neg q$ (§);

3.º, por $(*)$ y (§), concluimos que si se supone p, se sigue $\neg q$ y $\neg r$.

Ejemplo 167

> «Utilizaremos ambas componentes software sólo si a igual número de peticiones su capacidad de respuesta es la misma. Cuidado, insistimos, que el número de peticiones sea el mismo, no sólo que respondan por igual. Pero entonces, de todo lo anterior, se deduce que no es cierto que se vayan a utilizar ambas componentes».
>
> [EPF 14.5.2019:1b1] (por tablas semánticas).

Resolución.— En el ejemplo 97 (pág. 137 de esta edición) resolvimos esta argumentación por tablas de verdad.

0. y 1. En dicho ejemplo resolvimos los apartados 0 y 1 que aquí se piden, esto es:

   - hallamos el argumento $\mathcal{A}$ correspondiente;
   - propusimos su formalización (variables proposicionales, esquema argumental y forma lógica) en lógica de juntores;
   - identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{p \rightarrow (q \rightarrow r), q \wedge r\}$ y la conclusión ψ, a saber, $\neg p$;
   - sugerimos la forma lógica en lógica de juntores para $\mathcal{A}$, que resultó ser $(p \rightarrow (q \rightarrow r)) \wedge q \wedge r \rightarrow \neg p$.

   Ahora, en este ejemplo, nos preguntamos si $(p \rightarrow (q \rightarrow r)) \wedge q \wedge r \rightarrow \neg p$ es una fórmula válida, en otras palabras, si se satisface $(p \rightarrow (q \rightarrow r)), q \wedge r \vDash \neg p$.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1\} \vDash \psi$. Refutar $\{\phi_0, \phi_1\} \vDash \psi$ es demostrar que $\phi_0 \wedge \phi_1 \wedge \neg\psi$ es una fórmula válida.

   Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0, \phi_1\} \cup \{\neg\psi\} = \{p \rightarrow (q \rightarrow r), q \wedge r, p\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico.*

   Veamos el árbol generado por *logic-rs* en la figura 3.1 (pág. 326 de esta edición).

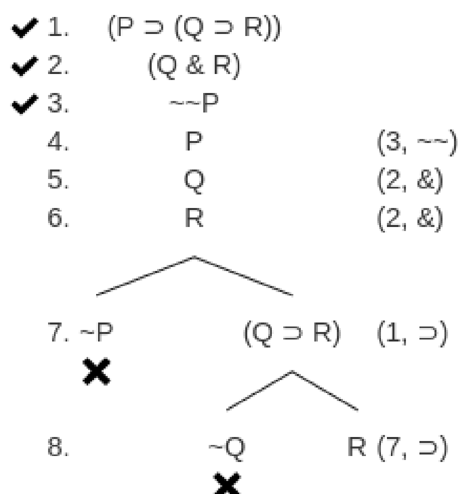


Figura 3.1.—Árbol semántico correspondiente a Γ que genera el artefacto en línea *logic-rs* con la entrada `(P ⊃ (Q ⊃ R)),` (en la línea 1), `(Q & R),` (en la línea 2) y `P` (en la línea 3 ∴) (el uso de las mayúsculas latinas es una imposición de *logic-rs*). La notación es la de Lepore y Cumming [94].

Actividad 3.4

Como vemos, este artefacto en línea utiliza otra notación para anotar el árbol; por un lado, entendámosla, por otro, anotémoslo convenientemente utilizando nuestra notación habitual.

III. *Demostración de que es un árbol terminado.*

El tronco ρ_0 de este árbol es $\rho_0 = \langle (p \to (q \to r)) \land (q \land r), \neg\neg p, p \to (q \to r), q \land r, q, r, p \rangle$; tiene, además, tres ramas:
$\rho_1 = \rho_0 +\!\!+ \langle \neg p \rangle$;
$\rho_2 = \rho_0 +\!\!+ \langle q \to r, \neg q \rangle$;
$\rho_3 = \rho_0 +\!\!+ \langle q \to r, r \rangle$.

Es un árbol terminado, pues toda rama es insatisfactible o completa. En efecto:

- por un lado, ρ_1 y ρ_2 son ramas insatisfactibles, al existir en cada una de ellas una variable y su negación: p y $\neg p$ en ρ_1 y q y $\neg q$ en ρ_2;
- por otro, ρ_3,
    - es una rama satisfactible, ya que corresponde a un conjunto satisfactible de fbf,
    - también es una rama completa, en efecto, comprobemos que si una fbf conjuntiva (de tipo α) pertenece a ρ_3, entonces también pertenecen a ρ_3 sus dos conjuntos y que si una fbf disyuntiva (de tipo β) pertenece a ρ_3, entonces también pertenece a ρ_3 alguno de sus disyuntos:

- con respecto a la fbf conjuntiva $\neg((p \to (q \to r)) \wedge (q \wedge r) \to (\neg p))$ (nodo 1), tanto $(p \to (q \to r)) \wedge (q \wedge r)$ como $\neg(\neg p)$ pertenecen al tronco ρ_0 (nodos 2 y 3, respectivamente) y por tanto, pertenecen a ρ_3;
- con respecto a la fbf conjuntiva $(p \to (q \to r)) \wedge (q \wedge r)$ (nodo 2), tanto $p \to (q \to r)$ como $q \wedge r$ pertenecen al tronco ρ_0 (nodos 4 y 5, respectivamente) y por tanto, pertenecen a ρ_3;
- con respecto a la fbf conjuntiva $\neg\neg p$ (nodo 3), $p \in \rho_0 \subset \rho_3$ (nodo 8);
- con respecto a la fbf disyuntiva $p \to (q \to r)$ (nodo 4), $(q \to r) \in \rho_3$ (nodo 10);
- con respecto a la fbf conjuntiva $q \wedge r$ (nodo 5), tanto q como r pertenecen al tronco ρ_0 (nodos 6 y 7, respectivamente) y, por tanto, a ρ_3;
- finalmente, con respecto a la fbf disyuntiva $q \to r$ (nodo 10), $r \in \rho_3$ (nodo 12).

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existe una rama satisfactible, ρ_3, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), de $p \to (q \to r)$ y $q \wedge r$, no se deduce $\neg p$, esto es, el argumento $\mathcal{A}$ no es válido e, igualmente, tampoco es válida la argumentación correspondiente.

3. *Identificación de los modelos que proporcionan las ramas satisfactibles.*

Al ser ρ_3 una rama satisfactible, proporciona un modelo para Γ, a saber,

$$I(p) = 1, I(q) = 1, I(r) = 1, \tag{3.5}$$

o en formato abreviado I_{111}. Y como es la única rama satisfactible, éste es el único modelo para Γ.

4. *Demostración de que los modelos lo son para Γ.*

No es difícil demostrar que I_{111} es un modelo para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dicha interpretación:

p	q	r	p	→	(q	→	r)	q	∧	r	p
1	1	1	1	[1]	1	1	1	1	[1]	1	[1]

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

De aquí que pueda refutarse $\mathcal{A}$, ya que el hecho de que vayamos a utilizar ambas componentes y que estas reciban igual número de peticiones cada una y que ambas respondan por igual, es suficiente para que se satisfaga las hipótesis y no se satisfaga la tesis y en definitiva, $\mathcal{A}$ no sea válido e, igualmente, tampoco sea válida la argumentación correspondiente.

- *Contraargumentación proporcionada por I_{111}*: Si utilizamos ambas componentes software y si ambas componentes software reciben igual número de peticiones y ambas componentes software tienen la misma capacidad de respuesta, entonces: por una parte, se satisface la primera premisa, pues se trata de implicaciones en las que los antecedentes y los consecuentes son verdaderos; por otra, se satisface la segunda premisa al ser la conjunción de satisfacerse que ambas componentes software reciben igual número de peticiones y que ambas tienen la misma capacidad de respuesta; pero lo que no se satisface es la conclusión, a saber, que no utilizamos ambas componentes software, puesto que sí las utilizamos. ■

Ejemplo 168

«Este programa compilará siempre que hayamos declarado las variables. Eso sí, declararemos las variables precisamente si no se nos olvida hacerlo. Resulta que el programa no ha compilado. Entonces es que hemos olvidado declarar las variables».

[SEL 3:9].

Resolución.—

0. *Argumento* ($\mathcal{A}$): Si hemos declarado las variables, entonces este programa compila. Si hemos declarado las variables, entonces no olvidamos declarar las variables, y recíprocamente. Este programa no ha compilado. Luego, olvidamos declarar las variables.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

   - *Variables proposicionales*.

     Siendo el universo de discurso el conjunto unión del de todos los programas y del de todos los signos lingüísticos, consideramos las siguientes variables proposicionales y las proposiciones simples que representan (y tomándonos la licencia de designar a aquéllas como a éstas, con letras latinas mayúsculas):

     $C \risingdotseq$ este programa compila,
     $D \risingdotseq$ hemos declarado las variables,
     $O \risingdotseq$ olvidamos declarar las variables.

   - *Esquema argumental*:

     Si se supone D, se sigue C.
     Si se supone D, se sigue no O, y recíprocamente.
     Se tiene no C.

     $\therefore$ Se sigue O.

- *Forma lógica.*

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2\} = \{D \to C, D \leftrightarrow \neg O, \neg C\}$ y la conclusión ψ, a saber, O.

  La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es

  $$(D \to C) \land (D \leftrightarrow \neg O) \land \neg C \to O.$$

  Llamémosla A.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1, \phi_2\} \vDash \psi$. Refutar $\{\phi_0, \phi_1, \phi_2\} \vDash \psi$ es demostrar que $\phi_0 \land \phi_1 \land \phi_2 \land \neg\psi$ es una fórmula válida.

   Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0, \phi_1, \phi_2\} \cup \{\neg\psi\} = \{D \to C, D \leftrightarrow \neg O, \neg C, \neg O\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico.*

   Veamos el árbol generado por pytableaux en la figura 3.2 (pág. 329 de esta edición).

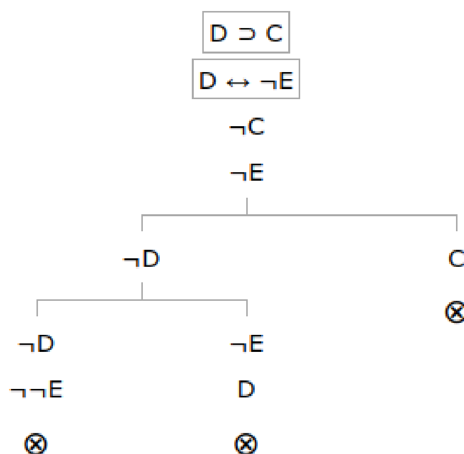


Figura 3.2.—Árbol semántico correspondiente a Γ que genera el artefacto en línea pytableaux con la entrada D > C (en P1), D % ~ E (en P2), C (en P3) y E (en C) (hemos sustituido O por E, ya que O es una letra reservada en pytableaux).

> **Actividad 3.5**
>
> Como vemos, este artefacto en línea construye el árbol prácticamente sin anotar (sólo las marcas de ramas insatisfactibles); anotémoslo convenientemente.

III. *Demostración de que es un árbol terminado.*

Este árbol tiene el tronco ρ_0 de nodos iniciales comunes,

$$\rho_0 = \langle D \to C, D \leftrightarrow \neg O, \neg C, \neg O \rangle,$$

y las tres ramas:

$\rho_1 = \rho_0 +\!\!+ \langle \neg D, O \rangle$;
$\rho_2 = \rho_0 +\!\!+ \langle \neg D, \neg O, D \rangle$;
$\rho_3 = \rho_0 +\!\!+ \langle C \rangle$.

Es un árbol terminado, pues toda rama es insatisfactible al existir en cada una de ellas al menos una variable y su negación:

- O y $\neg O$ en ρ_1;
- D y $\neg D$ en ρ_2, y
- C y $\neg C$ en ρ_3.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como todas las ramas son insatisfactibles, este árbol terminado es insatisfactible, por lo que hemos demostrado que Γ es un conjunto insatisfactible de fórmulas, en otras palabras, hemos encontrado una refutación para Γ, esto es, para $\Phi \cup \{\neg \psi\}$, lo cual, por el teorema 3.8 (pág. 281 de esta edición), sabemos que es equivalente a que $\Phi \vDash \psi$, es decir, a que ψ sea consecuencia lógica de Φ, en otras palabras, a que $\mathcal{A}$ sea un argumento válido e, igualmente, sea válida la argumentación correspondiente.

3. No procede (no hay ramas satisfactibles).
4. No procede (no hay modelos para Γ).
5. No procede (no hay contraargumentaciones). ■

Ejemplo 169

«No lo haré si tú no lo haces también. Pero tú no lo harás, a menos que yo lo apruebe. Por tanto, lo haremos si yo lo apruebo».

[AIC 10.4.2019:1].

Resolución.—

0. *Argumento.*
   - *Reescritura de la argumentación.*

Comencemos reescribiendo la argumentación para intentar aclarar su significado además de para acercarlo a patrones más sencillos de traducción de los conectores de la lógica de juntores, identificando las premisas y la conclusión.

Identificamos tres oraciones enunciativas:

I. «no lo haré si tú no lo haces también» ($\mathcal{O}_1$), en la que identificamos «no lo haré» ($\mathcal{O}_{1a}$) ($\neg p$) y «tú no lo haces» ($\mathcal{O}_{1b}$) ($\neg q$), unidas por «si» ($\mathcal{O}_{1a}$ si $\mathcal{O}_{1b}$), por lo que formalizamos $\mathcal{O}_1$ como «si $\mathcal{O}_{1b}$, entonces $\mathcal{O}_{1a}$»;

II. «tú no lo harás, a menos que yo lo apruebe» ($\mathcal{O}_2$), en la que identificamos «tú no lo harás» ($\mathcal{O}_{2a}$) y «yo lo apruebo» ($\mathcal{O}_{2b}$), unidas por «a menos que», por lo que formalizamos $\mathcal{O}_2$ como «si no $\mathcal{O}_{2b}$, entonces $\mathcal{O}_{2a}$»;

III. «lo haremos si yo lo apruebo» ($\mathcal{O}_3$), en la que identificamos «yo lo apruebo» ($\mathcal{O}_{3a}$) y «lo hagamos tú y yo» ($\mathcal{O}_{3b}$), formulando aquélla una condición suficiente para que se satisfaga ésta, que es por lo que formalizamos $\mathcal{O}_3$ como «si $\mathcal{O}_{3a}$, entonces $\mathcal{O}_{3b}$».

- *Argumento* ($\mathcal{A}$): Si tú no lo haces, entonces yo no lo hago. Si yo no lo apruebo, entonces tú no lo haces. Luego, si yo lo apruebo, entonces lo hacemos tú y yo.

1. *Formalización de $\mathcal{A}$ en lógica de juntores*.

- *Variables proposicionales*.

  Siendo el universo de discurso el conjunto de todas las personas, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

  p : «Yo lo hago»,
  q : «Tú lo haces»,
  r : «Yo lo apruebo».

- *Estructura lógico-gramatical*.

  Vista parcialmente a la hora de reescribir la argumentación. Con las variables anteriores, formalizamos en el lenguaje de la lógica de juntores, lo concluido allí en I, II y III, respectivamente, por: I, $\neg q \to \neg p$; II, $\neg r \to \neg q$, y III, $r \to (p \wedge q)$.

- *Esquema argumental*:

  Si se supone no q, se sigue no p.
  Si se supone no r, se sigue no q, y recíprocamente.
  ∴ Se sigue que si se supone r, se sigue p y q.

- *Forma lógica*.

Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{\neg q \to \neg p, \neg r \to \neg q\}$ y la conclusión ψ, a saber, $r \to (p \wedge q)$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(\neg q \to \neg p) \wedge (\neg r \to \neg q) \to (r \to (p \wedge q))$. Llamémosla A.

2. *Demostración de la validez o no de $\mathcal{A}$ mediante la estrategia de árboles semánticos.*

   I. *Identificación del conjunto Γ.*

   De acuerdo con la libertad que expone la nota de la entradilla de este apartado (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1\} \vDash \psi$. Refutar $\{\phi_0, \phi_1\} \vDash \psi$ es demostrar que $\phi_0 \wedge \phi_1 \wedge \neg\psi$ es una fórmula válida.

   Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0, \phi_1\} \cup \{\neg\psi\} = \{\neg q \to \neg p, \neg r \to \neg q, \neg(r \to (p \wedge q))\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

   II. *Construcción anotada del árbol semántico.*

   Veamos el árbol generado por Tree Proof Generator en la figura 3.3 (pág. 332 de esta edición).

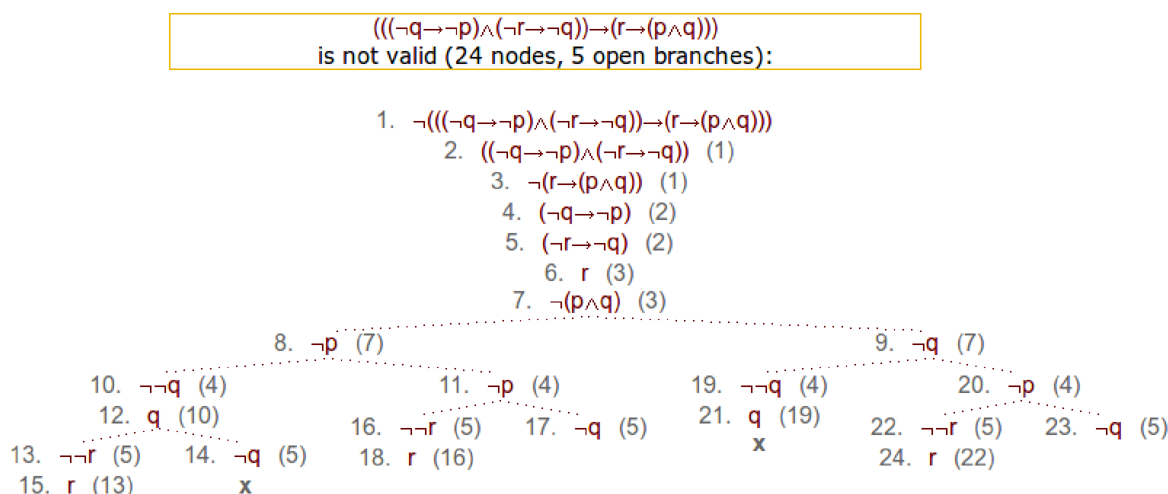


Figura 3.3.—Árbol semántico correspondiente a Γ que genera el artefacto en línea Tree Proof Generator (versión *oldtrees*) con la entrada `((\lnot q \to \lnot p) \wedge (\lnot r \to \lnot q)) \to (r \to (p \wedge q))`.

Actividad 3.6

Como vemos, este artefacto en línea construye el árbol con una anotación incompleta; anotémoslo convenientemente.

   III. *Demostración de que es un árbol terminado.*

El tronco ρ_0 de este árbol es $\rho_0 = \langle \neg((\neg q \to \neg p) \wedge (\neg r \to \neg q) \to (r \to (p \wedge q))), (\neg q \to \neg p) \wedge (\neg r \to \neg q), \neg(r \to (p \wedge q)), \neg q \to \neg p, \neg r \to \neg q, r, \neg(p \wedge q)\rangle$ y sus siete ramas son:

$\rho_1 = \rho_0 ++ \langle \neg p, q, r\rangle$,
$\rho_2 = \rho_0 ++ \langle \neg p, q, \neg q\rangle$,
$\rho_3 = \rho_0 ++ \langle \neg p, \neg p, r\rangle$,
$\rho_4 = \rho_0 ++ \langle \neg p, \neg p, \neg q\rangle$,
$\rho_5 = \rho_0 ++ \langle \neg q, q\rangle$,
$\rho_6 = \rho_0 ++ \langle \neg q, \neg p, r\rangle$,
$\rho_7 = \rho_0 ++ \langle \neg q, \neg p, \neg q\rangle$.

Es un árbol terminado, pues toda rama es insatisfactible o completa. En efecto:

- por un lado, ρ_2 y ρ_5 son ramas insatisfactibles, al existir en cada una de ellas una variable y su negación: q (nodos 12 en ρ_2 y 21 en ρ_5) y $\neg q$ (nodos 14 en ρ_2 y 9 en ρ_5) pertenecen a ρ_2 y ρ_5;
- por otro, ρ_1, ρ_3, ρ_4, ρ_6 y ρ_7 son ramas satisfactibles, pero completas:
    - con respecto a $(\neg q \to \neg p) \wedge (\neg r \to \neg q)$, tanto $\neg q \to \neg p$ como $\neg r \to \neg q$ forman parte del tronco ρ_0 y por tanto, pertenecen a todas las ramas;
    - con respecto a $\neg(r \to (p \wedge q))$, tanto r como $\neg(p \wedge q)$ forman parte del tronco ρ_0 y por tanto, pertenecen a todas las ramas;
    - con respecto a $\neg q \to \neg p$, $\neg p$ pertenece a las cinco ramas;
    - con respecto a $\neg r \to \neg q$, r pertenece a ρ_1 y a ρ_3 y $\neg q$ pertenece a ρ_4, ρ_6 y a ρ_7;
    - finalmente, con respecto a $\neg(p \wedge q)$, $\neg p$ pertenece a las cinco ramas.

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como existen ramas satisfactibles (cinco, para ser exactos: ρ_1, ρ_3, ρ_4, ρ_6 y ρ_7), este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), de $\neg q \to \neg p$ y $\neg r \to \neg q$, no se deduce $r \to (p \wedge q)$, de donde, el argumento $\mathcal{A}$ no es válido e, igualmente, no es válida la argumentación correspondiente.

3. *Identificación de los modelos que proporcionan las ramas satisfactibles.*

Al ser ρ_1, ρ_3, ρ_4, ρ_6 y ρ_7 ramas satisfactibles, proporcionan modelos para el conjunto de fórmulas bien formadas Γ, a saber:

- ρ_1 proporciona: $I(p) = 0$, $I(q) = 1$ e $I(r) = 1$;
- ρ_3 proporciona dos modelos:
    - $I(p) = 0$, $I(q) = 0$ e $I(r) = 1$;

- $I(p) = 0$, $I(q) = 1$ e $I(r) = 1$;

- ρ_4 proporciona: $I(p) = 0$, $I(q) = 0$ e $I(r) = 1$;
- ρ_6 proporciona: $I(p) = 0$, $I(q) = 0$ e $I(r) = 1$;
- ρ_7 proporciona: $I(p) = 0$, $I(q) = 0$ e $I(r) = 1$.

En definitiva, hay dos modelos para Γ:

0. $I(p) = 0$, $I(q) = 1$ e $I(r) = 1$, abreviadamente, I_{011} (proporcionado por ρ_1 y ρ_3), y
1. $I(p) = 0$, $I(q) = 0$ e $I(r) = 1$, abreviadamente I_{001} (proporcionado por ρ_3, ρ_4, ρ_6 y ρ_7).

4. *Demostración de que los modelos lo son para* Γ.

No es difícil demostrar que I_{011} e I_{001} son modelos para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dichas interpretaciones:

p q r	¬ q → ¬ p	¬ r → ¬ q	¬ (r → (p ∧ q))
0 1 1	0 1 [1] 1 0	0 1 [1] 0 1	[1] 1 0 0 0 1
0 0 1	1 0 [1] 1 0	0 1 [1] 1 0	[1] 1 0 0 0 0

5. *Expresión en español de las contraargumentaciones proporcionadas por los modelos*.

Es posible elaborar contraargumentos y contraargumentaciones:

- I_{011} proporciona:
  - *Contraargumento*: Si yo no lo hago y tú sí lo haces y yo lo apruebo, entonces: por una parte, se satisface la primera premisa, pues se trata de una implicación con antecedente (tú no lo haces) falso, ya que tú sí lo haces; por otra, se satisface la segunda premisa por un motivo similar, el antecedente (yo no lo apruebo) de la implicación es falso, puesto que sí lo apruebo; pero lo que no se satisface es la conclusión, ya que se trata de una implicación falsa, ya que su antecedente (yo lo apruebo) es verdadero y su consecuente (yo lo hago y tú lo haces) es falso, puesto que yo no lo hago.
  - *Contraargumentación*: Que yo lo apruebe y tú lo hayas hecho pero yo no, es suficiente para que no se satisfaga el argumento, pues aunque lo he aprobado no es cierto que tú lo hayas hecho y yo también.
- I_{001} proporciona:
  - *Contraargumento*: Si yo no lo hago y tú no lo haces y yo lo apruebo, entonces: por una parte, se satisface la primera premisa, pues se trata de una implicación con antecedente (tú no lo haces) verdadero y consecuente (yo no lo hago) verdadero; por otra, se satisface la segunda premisa, ya que el antecedente (yo no lo apruebo) de la implicación es falso, puesto que sí lo apruebo; pero lo que no se satisface es la conclusión, ya

que se trata de una implicación falsa, ya que su antecedente (yo lo apruebo) es verdadero y su consecuente (yo lo hago y tú lo haces) es falso, puesto que yo no lo hago ni tú lo haces.

- *Contraargumentación*: Que yo lo apruebe pero ni tú ni yo lo hayamos hecho, es suficiente para que no se satisfaga el argumento, pues aunque lo he aprobado no es cierto que tú lo hayas hecho y yo también. ■

Ejemplo 170

Utilicemos tablas de verdad como estrategia de refutación para comprobar que los resultados obtenidos en los apartados segundo y tercero de la resolución del ejemplo anterior son correctos.

[AIC 10.4.2019:4a].

Resolución.— Al usar tabla de verdad como estrategia de refutación suponemos que la conclusión $r \rightarrow (p \wedge q)$ es falsa, de donde, por definición de implicador, el valor de verdad de r necesariamente es 1 y la «∧» es falsa; de esto último deducimos que p y q no pueden ser verdaderas a la vez; en resumen, en las interpretaciones de la tabla de verdad usada como estrategia de refutación, el valor de verdad de r es constantemente 1 y los de p y q pueden 1 o 0 pero no 1 a la vez. Mostramos a continuación dicha tabla.

p	q	r	$((\neg$	q	$\rightarrow$	$\neg$	$p)$	$\wedge$	$(\neg$	r	$\rightarrow$	$\neg$	$q))$	$\rightarrow$	$(r$	$\rightarrow$	$(p$	$\wedge$	$q))$	
1	0	**1**	1	0	0	0	1			**1**					**1**	0		0		✗
0	1	**1**	0	1	[1]	1	0		0	**1**	[1]	0	1		**1**	[0]	0	0	1	✓
0	0	**1**	1	0	[1]	1	0		0	**1**	[1]	1	0		**1**	[0]	0	0	0	✓

Recordemos que nuestra búsqueda se basa en el hecho de que las hipótesis deben ser verdaderas y la conclusión falsa; así rechazamos la primera interpretación posible porque la primera hipótesis es falsa. ■

Ejemplo 171

La matemática explica el universo por ser éste matemático o por ser matemática la expresión de su existencia. Si lo explica por ser matemático, entonces toda emergencia es pura reducción, siendo cualquier razonamiento mera intuición. En cambio, si tal explicación es por ser matemática la expresión de su existencia, no toda emergencia es pura reducción, existiendo además razonamientos no intuitivos. La matemática hace de toda emergencia pura reducción, a no ser que cualquier razonamiento sea mera intuición. Por lo tanto, no es cierto que la matemática haga de toda emergencia pura reducción sólo si existen razonamientos no intuitivos.

Resolución.— (Inicio).

0. *Argumento* ($\mathcal{A}$): La matemática explica el universo por ser éste matemático o la matemática explica el universo por ser matemática la expresión de su existencia o ambas cosas. Si la matemática explica el universo por ser éste matemático, entonces la matemática hace que toda emergencia sea pura reducción y que no existan razonamientos no intuitivos. Si la matemática explica el universo por ser matemática la expresión de su existencia, entonces la matemática hace que no toda emergencia sea pura reducción y la matemática hace que existan razonamientos no intuitivos. Es falso que la matemática no haga que toda emergencia sea pura reducción y simultáneamente haga que existan razonamientos no intuitivos. Por lo tanto, es falso que la matemática haga que toda emergencia es pura reducción sólo si hace que existan razonamientos no intuitivos.

1. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales.*

     Siendo el universo de discurso el universo, consideramos las siguientes variables proposicionales y las proposiciones simples que representan:

     $p \leftrightharpoons$ la matemática explica el universo por ser éste matemático;
     $q \leftrightharpoons$ la matemática explica el universo por ser matemática la expresión de su existencia;
     $r \leftrightharpoons$ la matemática hace que toda emergencia sea pura reducción;
     $s \leftrightharpoons$ la matemática hace que existan razonamientos no intuitivos.

- *Esquema argumental*:

	Se tiene p o q.
	Si se supone p, se sigue r y no s.
	Si se supone q, se sigue no r y s.
	Se tiene la falsedad de la conjunción de no r y s.
∴	Se sigue la falsedad de que si se supone r, se sigue la falsedad de no s.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2, \phi_3\} = \{p \vee q, p \rightarrow r \wedge \neg s, q \rightarrow \neg r \wedge s, \neg(\neg r \wedge s)\}$ y la conclusión ψ, a saber, $\neg(r \rightarrow \neg\neg s)$.

  La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es

$$(p \vee q) \wedge (p \rightarrow r \wedge \neg s) \wedge (q \rightarrow \neg r \wedge s) \wedge \neg(\neg r \wedge s) \rightarrow \neg(r \rightarrow \neg\neg s).$$

  Llamémosla A.

✍.— Continúa en la actividad 3.21 (pág. 342 de esta edición). ■

§ 3.4 Propuesta de más actividades

Proponemos las cuestiones aquí agrupadas como entrenadoras de la estrategia de tablas analíticas/semánticas. Sin embargo, sería un buen trabajo aplicar tanto las diferentes estrategias estudiadas hasta este momento como las que están aún por conocer. Es por esto que deberíamos volver aquí durante el estudio futuro.

Actividad 3.7

Utilizando TA/S demostremos que la siguiente es una fórmula válida —es el llamado *praeclarum theorema* [teorema espléndido] por Leibniz—.

$$(\phi \rightarrow \chi) \wedge (\psi \rightarrow \tau) \rightarrow (\phi \wedge \psi \rightarrow \chi \wedge \tau).$$

Aunque ya hemos razonado diagramáticamente (*cfr. supra* ejemplo 100 [pág. 148 de esta edición])—, quienes gocemos de más inquietudes y tiempo para satisfacerlas pudiésemos asomarnos aún más al *razonamiento diagramático* y ver una demostración del teorema esplén-

dido —allí llamado «brillante»— mediante los *gráficos existenciales alfa* de PEIRCE (*vid. v. gr.* https://es.wikipedia.org/wiki/Razonamiento_diagramático).

Actividad 3.8

Utilizando TA/S demostremos que la siguiente es una fórmula válida —es el dilema constructivo complejo (DCC)—:

$$(\phi \to \chi) \wedge (\psi \to \tau) \to (\phi \vee \psi \to \chi \vee \tau).$$

Actividad 3.9

Utilizando TA/S demostremos que las fórmulas recíprocas del teorema espléndido y del dilema constructivo complejo no son fórmulas válidas.

Actividad 3.10

Utilizando TA/S demostremos que $((\phi \wedge \psi) \to \chi) \leftrightarrow ((\neg\chi \wedge \phi) \to \neg\psi)$.

Actividad 3.11

Utilizando TA/S demostremos que $(\phi \to (\psi \vee \chi)) \leftrightarrow ((\phi \wedge \neg\psi) \to \chi)$.

Para todas y cada una de las afirmaciones o situaciones que proporcionan las siguientes actividades, hagamos lo mismo que en § 3.3.7 (pág. 283 de esta edición).

Actividad 3.12

«Dadas dos situaciones, del hecho de que ocurran ambas, siempre es posible inferir que ocurre alguna de ellas».

[Cubit 33], [SEL 3:2].

Con miras a su resolución.— Identificadas las situaciones como A y B y siendo $p \leftrightharpoons$ Sucede la situación A, y $q \leftrightharpoons$ Sucede la situación B, entonces la inferencia es $\{p \wedge q\} \vdash p \vee q$.

Actividad 3.13

«Lo hacen quienes piensan así y quienes trabajan allí. Aunque, en realidad, quienes trabajan allí lo hacen siempre que lo hacen quienes leen estas líneas. Por tanto, no es cierto que quienes piensan así lo hagan siempre que lo hagan quienes trabajan allí».

[SEL 3:8].

Con miras a su resolución.— Siendo $p \leftrightharpoons$ Lo hacen quienes piensan así, $q \leftrightharpoons$ Lo hacen quienes trabajan allí, y $r \leftrightharpoons$ Lo hacen quienes leen estas líneas, entonces la inferencia es $\{p \wedge q, r \rightarrow q\} \vdash \neg(q \rightarrow p)$.

Actividad 3.14

«El CIA (coeficiente de inteligencia artificial) permanece constante sólo si se incrementa la creatividad humana o no emerge la conciencia artificial. La creatividad humana crece a menos que las inteligencias artificiales consigan manipular al ser humano. Si el CIA permanece constante y las inteligencias artificiales consiguen manipular al ser humano, emerge la conciencia artificial. Por lo tanto, se incrementa la creatividad humana».

[Cubit 15], [PEP 14.4.2023:1].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $((p \rightarrow (q \vee \neg r)) \wedge (\neg q \rightarrow s) \wedge ((p \wedge s) \rightarrow r)) \rightarrow q$, donde las variables proposicionales son: $p \leftrightharpoons$ El CIA permanece constante; $q \leftrightharpoons$ Se incrementa la creatividad humana; $r \leftrightharpoons$ Emerge la conciencia artificial; $s \leftrightharpoons$ Las inteligencias artificiales consiguen manipular al ser humano. Es una contingencia. Pudiésemos utilizar el artefacto en línea The Truth Tree Solver[42] para ver la tabla semántica —la petición sería `not (((P then (Q or not R)) and (not Q then S) and ((P and S) then R)) then Q)` o bien `((P then (Q or not R)) and (not Q then S) and ((P and S) then R)) and not Q`—. En dicha tabla semántica, vemos que los modelos que proporcionan las ramas satisfactibles son los siguientes: ρ_3 proporciona los modelos $\langle p, q, r, s\rangle \leftarrow\!\shortmid \langle 0, 0, 0, 1\rangle$, abreviadamente I_{0001}, y $\langle p, q, r, s\rangle \leftarrow\!\shortmid \langle 0, 0, 1, 1\rangle$, abreviadamente I_{0011}; ρ_5 proporciona el modelo $\langle p, q, r, s\rangle \leftarrow\!\shortmid \langle 0, 0, 1, 1\rangle$, esto es, I_{0011}, y ρ_9 proporciona el modelo $\langle p, q, r, s\rangle \leftarrow\!\shortmid \langle 0, 0, 0, 1\rangle$, esto es, I_{0001}. Las expresiones en español de las contraargumentaciones proporcionadas por estos modelos son: ▪ Si el CIA varía y no se incrementa la creatividad humana y no emerge la conciencia artificial y las inteligencias artificiales consiguen manipular al ser humano, entonces se satisfacen las premisas pero no se satisface la conclusión —proporcionada por I_{0001}—, y ▪ Si el CIA varía y no se incrementa la creatividad humana y emerge la conciencia artificial y las inteligencias artificiales consiguen manipular al ser humano, entonces se satisfacen las premisas pero no se satisface la conclusión —proporcionada por I_{0011}—.

Actividad 3.15

«Si el hecho de que un gobierno tome unas medidas económicas arbitrarias y a la vez debilite los pilares fundamentales de la sociedad implica contradicciones sociales (por ejemplo, que dicho gobierno, elegido por la ciudadanía, no considere las demandas de la ciudadanía durante su legislatura), se deduce que caso de que un gobierno aplique unas medidas económicas arbitrarias debe reforzar los pilares fundamentales de la sociedad».

[SEL 3:4].

Con miras a su resolución.— Siendo $p \leftrightharpoons$ Un gobierno toma medidas económicas arbitrarias, y $q \leftrightharpoons$ Se refuerzan los pilares fundamentales de la sociedad, entonces la inferencia es $\{p \wedge \neg q \rightarrow \bot\} \vdash p \rightarrow q$.

[42] *Cfr. infra* § 3.3.9 (pág. 319 de esta edición).

Actividad 3.16

«Esta normativa será aprobada en esta sesión precisamente si es apoyada por la mayoría. Se sabe a ciencia cierta que o es apoyada por la mayoría o el equipo de gobierno se opone a ella, pero no ambas cosas. Si el equipo de gobierno se opone a ella, será propuesta para su revisión. Por tanto, o esta normativa será aprobada en esta sesión o será propuesta para su revisión o puede que ambas cosas».

Con miras a su resolución.— Siendo las premisas $p \leftrightarrow q$, $q \veebar r$, y $r \rightarrow t$, ¿es posible deducir $p \vee t$? Sabemos que $p \veebar q \leftrightarrow (p \vee q) \wedge (\neg p \vee \neg q)$ (regla CV) y también que $p \veebar q \leftrightarrow (p \wedge \neg q) \vee (\neg p \wedge q)$ (regla ICV$_2$). Por la primera, conformamos la deducción formal:

0.	$p \leftrightarrow q$	Premisa
1.	$q \veebar r$	Premisa
2.	$r \rightarrow t$	Premisa
3.	$(q \vee r) \wedge (\neg q \vee \neg r)$	CV 1
4.	$q \vee r$	EC$_0$ 3
5.	$q \rightarrow p$	ECO$_1$ 0
6.	$p \vee t$	DCC 4, 5, 2

donde DCC es la regla dilema constructivo complejo.

Actividad 3.17

«Yo dije que si había agua en la charca y estaba limpia, bebería de la charca y que si no estaba limpia el agua de la charca, bebería de la cantimplora. Así que, si no bebí ni de la charca ni de la cantimplora es que no había agua en la charca».

[SEL 3:11].

Con miras a su resolución.— Siendo $p \leftrightharpoons$ Hay agua en la charca, $q \leftrightharpoons$ El agua está limpia, y $r \leftrightharpoons$ Bebo de la charca, entonces la inferencia es $\{p \wedge q \rightarrow r, \neg q \rightarrow s\} \vdash \neg r \wedge \neg s \rightarrow \neg p$.

Actividad 3.18

«Los partidos políticos podrían trabajar conjuntamente para mayor provecho social, al menos durante un cierto tiempo, si se fundamentasen en la justicia, en la bondad y en la satisfacción comunitaria. Pero para que eso ocurriese, haría falta una educación que favoreciese lo comunitario, una experiencia comunitaria prepolítica y una emancipación con respecto a la individualidad y al egoismo. Ahora bien, estos mismos factores que son los que permitirían la existencia de partidos políticos que trabajasen conjuntamente para mayor provecho social, significan al propio tiempo su condena, su no necesidad. Luego, los partidos políticos no se fundamentan ni en la justicia ni en la bondad ni en la satisfacción comunitaria».

[SEL 3:12].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $(p \to q) \wedge (r \leftrightarrow p) \wedge (r \to (q \wedge \neg q)) \to \neg p$, donde las variables proposicionales son: $p \leftrightharpoons$ Los partidos políticos se fundamentan en la justicia, en la bondad y en la satisfacción comunitaria; $q \leftrightharpoons$ Los partidos políticos pueden trabajar conjuntamente para mayor provecho social; $r \leftrightharpoons$ La educación favorece lo comunitario, una experiencia comunitaria prepolítica y una emancipación con respecto a la individualidad y al egoismo. Pudiésemos utilizar el artefacto en línea The Truth Tree Solver[43] para ver la tabla semántica, con la petición `not (((P then Q) and (R equiv P) and (R then (Q and not Q))) then not P)` o bien con `((P then Q) and (R equiv P) and (R then (Q and not Q))) and not not P`; vemos que resulta un árbol de refutación para $\Gamma = \{p \to q, r \leftrightarrow p, r \to (q \wedge \neg q), \neg\neg p\}$, en otras palabras, la fórmula es válida y la argumentación también.

Actividad 3.19

Año 3210. Tres robots antropomorfos, P, Q y R, están bajo sospecha de un robo. Tras la investigación de la escena del delito, se ha determinado que:

0. ninguna entidad más que P, Q y R están bajo sospecha y al menos uno de ellos tres es el responsable del robo;
1. los robots P y R son indistinguibles a todos los efectos —tanto es así que en muchos cursos de introducción a la filosofía se les suele poner de contraejemplo de la identidad de los indiscernibles*—, además, ni P ni R jamás hacen nada sin la compañía del otro;
2. el robot Q, sin embargo, actúa siempre solo;
3. en el intervalo de tiempo que se ha estimado para el suceso, bien P bien R —no se sabe cuál debido a su indistinguibilidad—, fue visto en otro lugar.

¿Qué podemos concluir razonadamente? ¿Podremos encontrar al culpable o culpables? ¿Quién o quiénes? Utilicemos TA/S para la resolución.

* *Vid. infra* § 5.1 (pág. 406 de esta edición).

Actividad 3.20

«Un sistema operativo cuántico funciona en modo convencional o en modo abstracto. Si funciona en modo convencional, entonces muestra una interfaz intuitiva, pero el núcleo pierde la causalidad. Si funciona en modo abstracto, la interfaz intuitiva desaparece, pero el núcleo mantiene la causalidad. No es cierto que en un sistema operativo cuántico la interfaz intuitiva desaparezca y que el núcleo mantenga la causalidad. Por lo tanto, no es cierto que si un sistema operativo cuántico muestra una interfaz intuitiva, el núcleo no pierda la causalidad».

[Cubit 68].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $(p \vee q) \wedge (p \to (r \wedge \neg s)) \wedge (q \to (\neg r \wedge s)) \wedge \neg(\neg r \wedge s) \to \neg(r \to \neg\neg s)$, donde las

[43] *Vid. supra* § 3.3.9 (pág. 319 de esta edición).

variables proposicionales son: $p \leftrightharpoons$ El sistema operativo cuántico funciona en modo convencional; $q \leftrightharpoons$ El sistema operativo cuántico funciona en modo abstracto; $r \leftrightharpoons$ El sistema operativo cuántico muestra una interfaz intuitiva; $s \leftrightharpoons$ El núcleo mantiene la causalidad. Pudiésemos utilizar el artefacto en línea The Truth Tree Solver[44] para ver la tabla semántica, con la petición `not ((P or Q) and (P then (R and not S)) and (Q then (not R and S)) and not (not R and S) then not (R then not not S))` o bien con `(P or Q) and (P then (R and not S)) and (Q then (not R and S)) and not (not R and S) and not not (R then not not S)`; vemos que resulta un árbol de refutación para $\Gamma = \{p \vee q, p \to (r \wedge \neg s), q \to (\neg r \wedge s), \neg(\neg r \wedge s), \neg\neg(r \to \neg\neg s)\}$, en otras palabras, la fórmula es válida y la argumentación también.

Actividad 3.21

Completemos la resolución del ejemplo 171 (pág. 336 de esta edición). Como práctica, pudiésemos utilizar todos los artefactos estudiados en § 3.3.9 (pág. 319 de esta edición).

Con miras a su resolución.— Por ejemplo, con el artefacto The Truth Tree Solver, con la petición `not ((P or Q) and (P then (R and not S)) and (Q then (not R and S)) and not (not R and S) then not (R then not not S))` o bien con `(P or Q) and (P then (R and not S)) and (Q then (not R and S)) and not (not R and S) abd not (not (R then not not S))`.

Actividad 3.22

La tabla/árbol analítica/semántica (TA/S) de la fórmula $(p \to q) \wedge (r \to s) \wedge (t \to p) \wedge (r \vee t) \to (q \wedge s)$, en el que para su construcción hemos hecho uso en todo momento de la guía y heurística para la aplicación de las reglas de extensión, se trata de:

a. un árbol insatisfactible;
b. un árbol satisfactible con sólo una rama satisfactible;
c. un árbol satisfactible con sólo dos ramas satisfactibles;
d. un árbol satisfactible con sólo tres ramas satisfactibles.

[TT].

Actividad 3.23

La tabla/árbol analítica/semántica (TA/S) de la fórmula $(p \to q) \wedge (r \to s) \wedge (q \to t) \wedge (s \to u) \wedge (p \vee r) \to (t \vee u)$, en el que para su construcción hemos hecho uso en todo momento de la guía y heurística para la aplicación de las reglas de extensión, se trata de:

a. un árbol insatisfactible;
b. un árbol satisfactible con sólo una rama satisfactible;
c. un árbol satisfactible con sólo dos ramas satisfactibles;
d. un árbol satisfactible con sólo tres ramas satisfactibles.

[TT].

---

[44] *Vid. supra* § 3.3.9 (pág. 319 de esta edición).

§ 3.5 De la demostración

Nos hemos enfrentado a argumentaciones con un doble propósito en mente, demostrar su validez o su invalidez (refutarlas). En el primer caso, debemos verificarla y, por el momento, después de simplificada en argumento y de encontrado su esquema argumental, Premisas $\vdash$ Conclusión, y una vez traducido éste al lenguaje de la lógica de juntores, $(p_0 \wedge p_1 \wedge \ldots \wedge p_n) \rightarrow c$, podemos usar una o más de las estrategias de demostración estudiadas hasta el momento. No obstante, si lo que queremos es refutar la argumentación, debemos encontrar una contraargumentación. De nuevo, una vez la argumentación ha sido traducida al lenguaje de la lógica de juntores, pudiésemos aprovecharnos también de las tablas de verdad aunque ahora usándolas como estrategia de refutación, centrándonos en el hecho de que estamos buscando una contraargumentación, cosa que vamos a conseguir mediando un modelo para el conjunto Γ formado por las premisas y la negación de la conclusión, $= \{p_0, p_1, \ldots, p_n, \neg c\}$, pues dicho modelo es precisamente un contramodelo para $(p_0 \wedge p_1 \wedge \ldots \wedge p_n) \rightarrow c$, contramodelo que nos permitirá construir una contraargumentación.

Recordemos que una interpretación es una asignación de valores de verdad a las variables que participan en la formalización del argumento, que un modelo para una fórmula (fórmula bien formada, es decir, cualquier expresión en el lenguaje de la lógica que sea sintácticamente correcta) es cualquier interpretación que hace verdadera a la fórmula, y que un modelo para un conjunto de fórmulas es cualquier interpretación que sea un modelo para todas las fórmulas del conjunto, diciéndose en este último caso que el conjunto es satisfactible (o también consistente o posible).

Así, una argumentación no es válida si, y sólo si, la tabla de verdad de su correspondiente fórmula contiene al menos una interpretación que es un modelo para el conjunto formado por las premisas y la negación de la conclusión. En esto consiste utilizar

- las tablas de verdad como estrategia de verificación.

Como pudiésemos haber cometido un error al construir esta tabla de verdad, puede ser recomendable aplicar una estrategia adicional. Hemos visto varias de éstas:

- tablas de verdad como estrategia de refutación;
- tablas de verdad para demostrar la consistencia;
- reducción al absurdo (Abs, RAA) —estas dos últimas esquemáticamente, en un cuadro de cuatro filas: 0.ª, la fórmula; 1.ª, los valores de verdad (con una o más interpretaciones); 2.ª, pasos, y 3.ª, justificación de cada paso—;
- demostraciones por encadenamiento de equivalencias lógicas;
- formas normales (reglas FND y FNC);
- dualidad;

- derivaciones/deducciones formales (sintácticas);
- derivaciones/deducciones semánticas, y
- tablas (árboles) analíticas/semánticas.

En fin, nada nos salva de la posibilidad de cometer errores —de los que no lo olvidemos, se aprende, o mejor dicho, errores, sin los que no se aprende—. Lo que parece indudable es que obtener la misma conclusión por dos caminos distintos, al menos, aparentemente aumenta la confianza en la solución (además de profundizar en el estudio y asimilación de tales caminos).

De hecho, en cuanto las conozcamos, pudiésemos incorporar estrategias no necesariamente pertenecientes a la lógica. También habremos de tener en cuenta que no siempre tenemos por qué proporcionar una respuesta definitiva. Tengamos la seguridad de que la mayoría de quienes estudien nuestra respuesta nos agradecerán poder participar en la toma de decisión, además de que así les facilitamos poder entender los entresijos de la misma[45].

En fin, éstas han sido las primeras estrategias, métodos o técnicas de demostración. No olvidemos, por ejemplo, que hemos trabajado ya con demostraciones por casos y que cualquier regla de inferencia admite el punto de vista de ser una estrategia de demostración: *estrategia de modus ponens*, *estrategia de modus tollens*, *estrategia del dilema*, etc. A lo largo de estas páginas aprenderemos otras cuantas más. En el capítulo 7 (pág. 462 y ss. de esta edición) presentamos y analizamos algunas, sin ningún ánimo de exhaustividad.

Otros temas ligados a la argumentación y, por tanto, a la demostración, son los *paralogismos* y sus correspondientes en la lengua natural, las *falacias* —y entre éstas, los *sofismas*—, de los cuales estudiaremos algunos en el capítulo 8 (pág. 494 y ss. de esta edición). Mencionaremos las *paradojas*, si bien escasamente, a pesar de ser de interés computacional actual conocer cómo las inteligencias artificiales tratan de reconocerlas o evitarlas.

Temas pendientes para próximas revisiones o ediciones de estas notas son la *construcción automática de argumentos* (pensemos en una de tales inteligencias «leyendo» una novela de intriga que fuese fabricando un argumento para concluir la resolución del misterio) y la *reconstrucción de argumentos* —tan útil en los procesos judiciales— y las interrelaciones, interdependencias o entrelazamientos entre la *ética* y la lógica[46]. También de muchos otros temas interesantes relacionados con la lógica en su sentido amplio o sobre otras lógicas concretas, como la lógica modal o la lógica intuicionista[47], ellas tan afines a la computación.

Ah, y no nos olvidemos del libro *El juego de la lógica*[48], de Lewis CARROLL.

[45] A modo de ejemplo, esta respuesta «multimodelo» sobre previsión de tiempo atmosférico: https://www.meteoblue.com/es/tiempo/pronostico/multimodel/c%c3%a1ceres_espa%c3%b1a_2520611.
[46] *Vid. v. gr.* https://es.unesco.org/artificial-intelligence/ethics/cases.
[47] De la lógica intuicionista diremos algo en § 7.19 (pág. 490 de esta edición).
[48] *Vid. v. gr.* https://archive.org/details/gameoflogic00carruoft/mode/2up.

Actividad 3.24

Resolvamos por cuantas estrategias de las estudiadas podamos la argumentación «— Estamos de acuerdo en que da lo mismo utilizar cualquiera de estas dos componentes, A o B. — Sí, pero ya lo hemos discutido y también coincidimos en que da lo mismo utilizar B que utilizar sólo una de las dos, A, o B. — Ah, vale, entonces no utilizamos A, ¿verdad?».

[Cubit 40].

Con miras a su resolución.— Una forma lógica correspondiente a esta argumentación en la lógica de juntores es $(p \leftrightarrow q) \wedge (q \leftrightarrow \neg(p \leftrightarrow q)) \rightarrow \neg p$, donde las variables proposicionales son: $p \leftrightharpoons$ Utilizamos la componente A; $q \leftrightharpoons$ Utilizamos la componente B. Pudiésemos utilizar el artefacto en línea The Truth Tree Solver[49] para ver la tabla semántica, con la petición `not (((P equiv Q) and (Q equiv not (P equiv Q))) then not P)` o bien `((P equiv Q) and (Q equiv not (P equiv Q))) and not not P`; vemos que resulta un árbol de refutación para $\Gamma = \{p \leftrightarrow q, q \leftrightarrow \neg(p \leftrightarrow q), \neg\neg p\}$, en otras palabras, la fórmula es válida y la argumentación también.

Actividad 3.25

Resolvamos por cuantas estrategias de las estudiadas podamos el siguiente acertijo lógico. Se trata de tres dispositivos, digamos A, B y C, interconectados de cierta forma, y de que averigüemos cuáles funcionan y cuáles no:

0. Siempre que A funciona, B también.
1. O bien B o bien C funcionan siempre, pero nunca ambos a la vez.
2. Siempre, bien A, bien C, o ambos, funcionan.
3. Cuando C funciona, también funciona A.

[49] *Vid. supra* § 3.3.9 (pág. 319 de esta edición).

§ 3.6 Lógica combinacional

A diferencia de la electrónica analógica en la que existen un número infinito de estados potenciales de información, la idea en electrónica digital es trabajar con un número finito de estados. Si se trabaja con dos estados, se representan por dos niveles de tensión —niveles lógicos—, bajo (lógica negativa) y alto (lógica positiva), determinados en la práctica por rangos diferenciados de voltaje, empleándose para su estudio matemático como correspondientes los dígitos 0 y 1 y el concepto de *bit* —dígito binario—. De este modo, utilizando álgebra de Boole pueden realizarse operaciones complejas con las señales de entrada de forma mucho menos costosa que si de electrónica analógica se tratase.

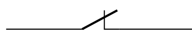
§ 3.6.0 Función booleana y circuito combinacional

Definición 3.15.— Una *función booleana* es una función $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$.

Un circuito lógico implementa una función booleana, siendo la aridad n de ésta, el número de señales de entrada del circuito. Distinguimos entre *circuitos combinacionales* y *circuitos secuenciales*. En los primeros, la salida depende sólo de las señales de entrada -son circuitos sin memoria—, mientras que los segundos tienen en cuenta entradas previas —son circuitos con memoria—. La *lógica combinacional* estudia los primeros y la *lógica secuencial* los segundos.

Un álgebra de Boole bivalorada suele denominarse *álgebra combinacional* o *álgebra de conmutación*. Esta álgebra proporciona las herramientas básicas para el diseño lógico de sistemas digitales, en concreto de *circuitos eléctricos combinacionales* —también llamados *circuitos de conmutación*—.

Fue Claude Shannon (1938) quien aplicó el cálculo lógico de juntores a la construcción de circuitos eléctricos combinacionales basados en *contactos* —también llamados *conmutadores* o *interruptores*—. En un circuito combinacional, todos los contactos son dispositivos de dos estados, por ejemplo, interruptores abiertos o cerrados y transistores con voltajes de salida bajo o alto: cerrado (encendido), permitiendo el paso de corriente,



y abierto (apagado),



no permitiendo el paso de corriente.

Suponemos que la corriente entra por la izquierda y se dirige hacia la derecha, por ejemplo, hacia una bombilla que se apagará, o encenderá según el estado de los contactos del circuito.

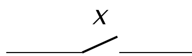
Utilizando la notación ordinaria de lógica de juntores podremos aplicar el *álgebra combinacional* a los circuitos eléctricos combinacionales. Para ello se etiqueta cada contacto con una variable pro-

posicional de forma que el contacto x está abierto precisamente si la variable x es 0 y el contacto x está cerrado si, y sólo si, la variable x es 1.

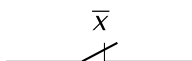
Resulta que es posible representar cada fórmula de la lógica de juntores mediante un circuito eléctrico combinacional, representando cada enunciado atómico mediante un circuito de un solo conmutador de dos estados, encendido —pasa la corriente– y apagado —no pasa la corriente—, y cada juntor diádico mediante una red de circuitos con conexiones apropiadas, en serie o paralelo. Por ejemplo, la conjunción de dos fórmulas se representa por un circuito de dos conmutadores conectados en serie, en otras palabras, la conexión en serie de dos circuitos monoconmutador.

Cada variable proposicional se representa por un interruptor, con dos posiciones: 0, abierto y 1, cerrado; la conexión en serie representa el juntor $\wedge$ y la conexión en paralelo, el juntor $\vee$; así, por ejemplo, un circuito que representa $p \wedge q$ —circuito AND— consiste en dos interruptores p y q conectados en serie, un circuito OR consiste en dos interruptores, p y q, conectados en paralelo y un circuito NOT es un circuito cerrado con un interruptor, p, que permite abrirlo. En los tres casos, la presión del interruptor representa la señal de entrada, mientras que el flujo de corriente por el circuito, la señal de salida. Así,

- el *buffer lógico* se representa por un circuito con un solo contacto x,

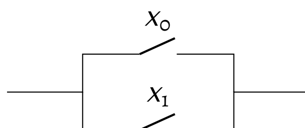


- el *inversor lógico* se representa por un circuito con un solo contacto $\overline{x}$,



  entendiendo que dicho contacto realiza una función inversa al contacto x del circuito correspondiente al buffer lógico, es decir, $\overline{x}$ estará abierto cuando x esté cerrado y viceversa;

- la *suma lógica* se representa por un circuito con dos contactos conectados en paralelo,



  circuito que permitirá el paso de corriente si, y sólo si, al menos uno de los contactos está cerrado;

- el *producto lógico* se representa por un circuito con dos contactos conectados en serie,



circuito que permitirá el paso de corriente si, y sólo si, sus dos contactos están cerrados.

Suelen utilizarse tablas de verdad para expresar las salidas de los circuitos combinacionales.

§ 3.6.1 Compuerta lógica

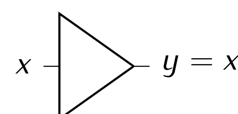
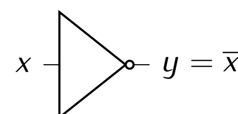
Los circuitos combinacionales más elementales se conocen como *compuertas/puertas lógicas* y se corresponden con los juntores de la lógica de juntores. Su notación es la que usamos en la *diagramática combinacional* a la que dedicamos este apartado.

Cualquier función booleana puede ser reescrita como una expresión booleana respecto de una base de operadores booleanos, notémoslos $\{', \sqcup, \sqcap\}$ o $\{', +, \cdot\}$. Esta expresión booleana proporciona una forma de implementar la función booleana con un circuito combinacional.

En los siguientes apartados mostramos diez compuertas lógicas. En horizontal, de izquierda a derecha, aparecen la expresión en lógica de juntores, la expresión booleana, el nombre, la expresión algebraica combinacional y tabla de verdad y, finalmente, el diagrama combinacional según el estándar ANSI/IEEE Std 91/91a-1991[50].

§ 3.6.2 Compuertas lógicas monádicas

Las compuertas buffer lógico e inversor lógico (NOT) corresponden a los juntores monádicos afirmación y negación, respectivamente.

x	x	Buffer lógico	$\begin{array}{c\|c} x & x \\ \hline 1 & 1 \\ 0 & 0 \end{array}$	
$\neg x$	x'	Inversor lógico NOT	$\begin{array}{c\|c} x & \overline{x} \\ \hline 1 & 0 \\ 0 & 1 \end{array}$	

[50] *Cfr. v. gr.* https://de.wikipedia.org/wiki/Logikgatter#Typen_von_Logikgattern_und_Symbolik para éste y otros estándares.

§ 3.6.3 Compuertas lógicas diádicas

Corresponden, respectivamente, a los juntores diádicos disyuntor, contravaledor, conjuntor, implicador, desimplicador, equivaledor, incompatibilizador y negador conjunto.

$x_0 \vee x_1$ $\quad$ $x_0 \sqcup x_1$ $\quad$ Compuerta lógica OR

$x_0 x_1$	$x_0 + x_1$
1 1	1
1 0	1
0 1	1
0 0	0

x_0, x_1 $\quad y = x_0 + x_1$

$x_0 \veebar x_1$ $\quad$ $x_0 \underline{\sqcup} x_1$ $\quad$ Compuerta lógica XOR/EXOR

$x_0 x_1$	$x_0 \oplus x_1$
1 1	0
1 0	1
0 1	1
0 0	0

x_0, x_1 $\quad y = x_0 \oplus x_1$

$x_0 \wedge x_1$ $\quad$ $x_0 \sqcap x_1$ $\quad$ Compuerta lógica AND

$x_0 x_1$	$x_0 \cdot x_1$
1 1	1
1 0	0
0 1	0
0 0	0

x_0, x_1 $\quad y = x_0 \cdot x_1$

$x_0 \to x_1$ $\quad$ $x_0' \sqcup x_1$ $\quad$ Compuerta lógica IMPLY

$x_0 x_1$	$x_0 \to x_1$
1 1	1
1 0	0
0 1	1
0 0	1

x_0, x_1 $\quad y = x_0 \to x_1$

$x_0 \wedge \neg x_1$ $\quad$ $x_0 \sqcap x_1'$ $\quad$ Compuerta lógica NIMPLY

$x_0 x_1$	$x_0 \cdot \overline{x}_1$
1 1	1
1 0	0
0 1	0
0 0	0

x_0, x_1 $\quad y = x_0 \cdot \overline{x}_1$

$x_0 \leftrightarrow x_1$ $\quad$ $(x_0 \underline{\sqcup} x_1)'$ $\quad$ Compuerta lógica XNOR/NEXOR

$x_0 x_1$	$x_0 \leftrightarrow x_1$
1 1	1
1 0	0
0 1	0
0 0	1

x_0, x_1 $\quad y = x_0 \leftrightarrow x_1$

$x_0 \overline{\wedge} x_1$ $\quad$ $x_0 \overline{\sqcap} x_1$ $\quad$ Compuerta lógica NAND

$x_0 x_1$	$x_0 \vert x_1$
1 1	0
1 0	1
0 1	1
0 0	1

x_0, x_1 $\quad y = x_0 | x_1$

$x_0 \overline{\vee} x_1$ $\quad$ $x_0 \overline{\sqcup} x_1$ $\quad$ Compuerta lógica NOR

$x_0 x_1$	$x_0 \downarrow x_1$
1 1	0
1 0	0
0 1	0
0 0	1

x_0, x_1 $\quad y = x_0 \downarrow x_1$

§ 3.6.4 Ejemplos de circuitos combinacionales

Como hemos dicho, varias compuertas lógicas pueden combinarse conformando un circuito combinacional. En el siguiente ejemplo mostramos la función booleana $\sqcup$, su reescritura como expresión booleana y como expresión algebraica combinacional y su representación como diagrama combinacional.

Ejemplo 172

La función booleana

$$\begin{array}{rccc} \sqcup : & \mathbb{Z}_2^2 & \longrightarrow & \mathbb{Z}_2 \\ & (1,1) & \longmapsto & 0 \\ & (1,0) & \longmapsto & 1 \\ & (0,1) & \longmapsto & 1 \\ & (0,0) & \longmapsto & 0 \end{array}$$

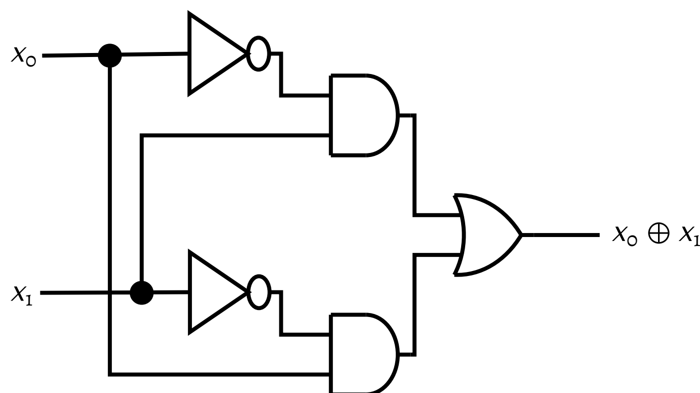
0. puede reescribirse como la expresión booleana

$$\begin{array}{rccc} \sqcup : & \mathbb{Z}_2^2 & \longrightarrow & \mathbb{Z}_2 \\ & (x_0, x_1) & \longmapsto & x_0 \sqcup x_1 = (x_0 \sqcap x_1{}') \sqcup (x_0{}' \sqcap x_1) \end{array}$$

1. puede reescribirse como la expresión algebraica combinacional

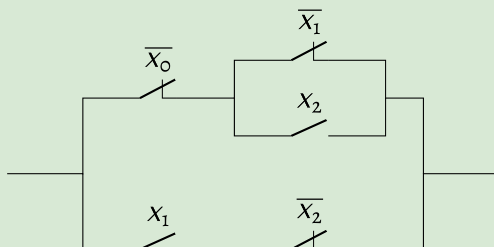
$$\begin{array}{rccc} \oplus : & \mathbb{Z}_2^2 & \longrightarrow & \mathbb{Z}_2 \\ & (x_0, x_1) & \longmapsto & x_0 \oplus x_1 = (x_0 \cdot \overline{x_1}) + (\overline{x_0} \cdot x_1) \end{array}$$

2. puede representarse con el diagrama combinacional



Ejemplo 173

¿Qué función booleana representa el siguiente circuito eléctrico combinacional?



Resolución.— Representa la función booleana

$$\begin{array}{rccl} f: & \mathbb{Z}_2^3 & \longrightarrow & \mathbb{Z}_2 \\ & \langle x_0, x_1, x_2 \rangle & \longmapsto & y = (\overline{x_0} \cdot (\overline{x_1} + x_2)) + (x_1 \cdot \overline{x_2}) \end{array}$$

■

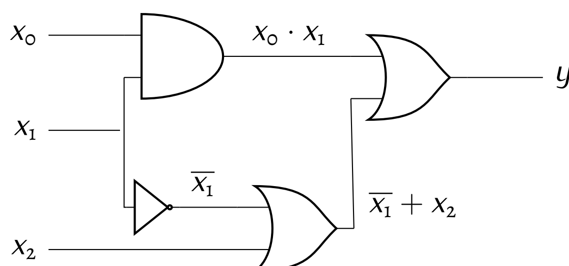
Ejemplo 174

Hallemos la tabla de verdad y un circuito que representen la función booleana

$$\begin{array}{rccl} f: & \mathbb{Z}_2^3 & \longrightarrow & \mathbb{Z}_2 \\ & \langle x_0, x_1, x_2 \rangle & \longmapsto & y = x_0 \cdot x_1 + (\overline{x_1} + x_2). \end{array}$$

Resolución.— Aquí están:

x_0	x_1	x_2	$y = x_0 \cdot x_1 + (\overline{x_1} + x_2)$
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	1



■

Actividad 3.26

Queremos diseñar un circuito para iluminar una señal de aviso si se presionan al menos dos de tres pulsadores.

Con miras a su resolución.— Sean p, q y r los tres pulsadores, cada uno con dos estados posibles: $0 \leftrightharpoons$ no pulsado, $1 \leftrightharpoons$ pulsado. La forma lógica correspondiente es $(\neg p \wedge q \wedge r) \vee (p \wedge \neg q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge q \wedge r)$, esto es, $(p \wedge q) \vee (p \wedge r) \vee (q \wedge r)$.

§ 3.6.5 Minimización de un circuito combinacional

Dada una función booleana, el objetivo es diseñar su computación mediante un circuito combinacional con el mínimo número de compuertas lógicas.

Lo estudiado en § 3.0 (pág. 256 de esta edición), en cuanto a simplificación de fórmulas tiene su utilidad aquí: simplificando la expresión de la función booleana en lógica de juntores, simplificaremos el circuito.

Definición 3.16.— En analogía con la lógica de juntores, decimos que un conjunto de compuertas lógicas $\{c_0, c_1, \ldots, c_k\}$ es una *base de compuertas lógicas* (bal) (o, sinónimamente, *conjunto adecuado de compuertas lógicas* [cal], *conjunto completamente expresivo de compuertas lógicas*, *conjunto completo de compuertas lógicas* o *conjunto funcionalmente completo de compuertas lógicas*) precisamente si para todo entero n y toda función booleana $f : \mathbb{Z}_2^n \longrightarrow \mathbb{Z}_2$ es posible construir un circuito combinacional que compute f usando sólo las compuertas $c_0, c_1, \ldots, c_k$.

Como estudiamos en el teorema 1.21 (pág. 164 de esta edición), las únicas bases de juntores minimales monádicas son $\{|\}$ y $\{\downarrow\}$, resultado que se traslada al presente ámbito estableciéndose como *las únicas bases de compuertas lógicas minimales monádicas* $\{\text{NAND}\}$ y $\{\text{NOR}\}$. De esta manera, dependiendo de la naturaleza del material utilizado pudiese incluso reducirse a implementar el circuito únicamente con compuertas NAND o únicamente con compuertas NOR. Las expresiones en lógica de juntores estudiadas en el ejemplo 107 (pág. 163 de esta edición), son de ayuda —por ejemplo, para generar NOT a partir de NAND o a partir de NOR, basta hacer única la entrada, esto es, $x_0 = x_1$ y así, $y = x_0|x_0 = \neg x_0$ e $y = x_0 \downarrow x_0 = \neg x_0$, respectivamente—.

Algunas renombradas y más compuertas lógicas

Por ejemplo: la *compuerta lógica inhibición* (INHIB), cuya expresión algebraica combinacional es $y = x_0 \cdot \overline{x}_1$ (esto es, la negación de IMPLY, $y = x_0 \nrightarrow x_1$); *compuertas lógicas inversas* (o, sinónimamente, *compuertas lógicas complementarias*), que se obtienen intercambiando $+$ y $\cdot$ y complementando las variables —por ejemplo, la *compuerta lógica inhibición inversa* (NINHIB), $y = \overline{x}_0 + x_1$, que no es más que IMPLY (igualmente que NOR es la inversa de OR, NAND la inversa de AND, XNOR la inversa de XOR y el inversor lógico la inversa del buffer lógico)—; la *compuerta lógica Votación* —si, y sólo si, suceden al menos m de las n entradas—, que si $n/2 < m$ también se conoce como la *compuerta lógica Mayoría* —por ejemplo, si $n = 3$ y $m = 2$, su ecuación booleana es $y = (x_0 \cdot x_1) + (x_0 \cdot x_2) + (x_1 \cdot x_2)$; *compuertas lógicas reversibles* como las de FEYNMAN[*], TOFFOLI[†], FREDKIN[‡] o PERES[§]; *compuertas lógicas cuánticas*[¶].

[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/Controlled_NOT_gate.
[†] *Vid. v. gr.* https://en.wikipedia.org/wiki/Toffoli_gate.
[‡] *Vid. v. gr.* https://en.wikipedia.org/wiki/Fredkin_gate.
[§] *Vid. v. gr.* https://en.wikipedia.org/wiki/List_of_quantum_logic_gates.
[¶] *Vid. v. gr.* https://en.wikipedia.org/wiki/Quantum_logic_gate.

§ 3.7 El álgebra de BOOLE de la lógica de juntores

§ 3.7.0 El álgebra de conmutación como álgebra de BOOLE

La suma lógica, el producto lógico y la complementación satisfacen unas determinadas propiedades que confieren al *álgebra de conmutación* $(\{0, 1\}; +, \cdot, ')$ de una estructura conocida como álgebra de BOOLE.

Estas propiedades son las siguientes.

La suma lógica y el producto lógico son operaciones

- asociativas, es decir, para todo x, y, z de $\{0, 1\}$,

$$(x + y) + z = x + (y + z),$$
$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$

- conmutativas, es decir, para todo x, y de $\{0, 1\}$,

$$x + y = y + x,$$
$$x \cdot y = y \cdot x,$$

- que satisfacen las leyes simplificativas la una respecto de la otra, es decir, para todo x, y de $\{0,1\}$,

$$x + (x \cdot y) = x,$$
$$x \cdot (x + y) = x,$$

además,

- son distributivas la una respecto de la otra, es decir, para todo x, y, z de $\{0,1\}$,

$$x + (y \cdot z) = (x + y) \cdot (x + z),$$
$$x \cdot (y + z) = (x \cdot y) + (x \cdot z),$$

y, aún más,

- ambas poseen elemento neutro, 0 es la identidad de la suma y 1 es la identidad del producto, esto es, para todo x de $\{0,1\}$, $0 + x = x$ y $1 \cdot x = x$:

$$0 + 0 = 0, \qquad 0 + 1 = 1,$$
$$1 \cdot 0 = 0, \qquad 1 \cdot 1 = 1,$$

- y todo elemento tiene su complementario, esto es, para todo x de $\{0,1\}$, $x + x' = 1$ y $x \cdot x' = 0$:

$$0 + 1 = 1, \qquad 1 + 0 = 1,$$
$$0 \cdot 0 = 0, \qquad 1 \cdot 0 = 0.$$

Decimos entonces que el álgebra de conmutación $(\{0,1\}; +, \cdot, ')$ del análisis de circuitos electrónicos combinacionales tiene estructura de *álgebra de* BOOLE o, simplemente, que es un álgebra de BOOLE.

§ 3.7.1 La estructura de álgebra de BOOLE

En § 17 (pág. 834 de esta edición), estudiaremos estructuras algebraicas en mayor amplitud y posicionaremos en ese marco el álgebra de BOOLE[51]. Baste en este punto, por razones de abstracción, que veamos tres definiciones (sólo tres, por razones de brevedad) de esta estructura algebraica.

Consideramos un conjunto B y cuatro operaciones definidas en él, $\sqcup$, $\sqcap$, $'$ y $\bullet$ —ejemplares de estas operaciones son, respectivamente, los juntores $\vee$, $\wedge$, $\neg$ y $\overline{\wedge}$, en el caso de la lógica, y la suma lógica, el producto lógico, la complementación y la negación del producto lógico (NAND), en el caso del álgebra de conmutación—.

[51] *Cfr. infra* § 17.12.5 (pág. 925 de esta edición).

Definición 3.17 (como *retículo distributivo y complementario*).— (Utiliza tres operaciones): $(B; \sqcup, \sqcap, ')$ es un álgebra de Boole si, y sólo si, para cualesquiera x, y, z de B,

0.°, $(B; \sqcup, \sqcap, ')$ es un *retículo*, es decir, se satisfacen las leyes

asociativas:
- de $\sqcup$: $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$,
- de $\sqcap$: $(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$,

conmutativas:
- de $\sqcup$: $x \sqcup y = y \sqcup x$,
- de $\sqcap$: $x \sqcap y = y \sqcap x$,

simplificativas/ de absorción:
- de $\sqcup$ respecto de $\sqcap$: $x \sqcup (x \sqcap y) = x$,
- de $\sqcap$ respecto de $\sqcup$: $x \sqcap (x \sqcup y) = x$;

1.°, $(B; \sqcup, \sqcap, ')$ es un *retículo distributivo*, es decir, se satisfacen (bastaría con que satisficiera una de las dos) las leyes

distributivas:
- de $\sqcup$ respecto de $\sqcap$: $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$,
- de $\sqcap$ respecto de $\sqcup$: $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$;

2.°, $(B; \sqcup, \sqcap, ')$ es un *retículo distributivo y complementado* (lo que supone ser acotado), es decir, satisface que existen los elementos neutros de $\sqcup$ y $\sqcap$ (acotado) y las leyes de complementación:

neutros:
- 0 es el de $\sqcup$: $0 \sqcup x = x$,
- 1 es el de $\sqcap$: $1 \sqcap x = x$,

complementación: existe x' de B, tal que
- $x \sqcup x' = 1$,
- $x \sqcap x' = 0$.

Definición 3.18 (de Huntington, 1933).— (Utiliza dos operaciones): $(B; \sqcup, ')$ es un álgebra de Boole si, y sólo si, para cualesquiera x, y, z de B,

0. $x \sqcup y = y \sqcup x$, ($\sqcup$ es conmutativa)

1. $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$, ($\sqcup$ es asociativa)

2. $(x' \sqcup y')' \sqcup (x' \sqcup y)' = x$. (axioma de Huntington)

Se define $\sqcap$ como *operación derivada* (también llamada *operación de segundo orden*), es decir, en función de las otras: $x \sqcap y = (x' \sqcup y')'$.

Definición 3.19 (de Wolfram, 2002).— (Utiliza sólo una operación): $(B; \bullet)$ es un álgebra de Boole si, y sólo si, para cualesquiera x, y, z de B,

$$((x \bullet y) \bullet z) \bullet (x \bullet ((x \bullet z) \bullet x)) = z,$$

definiéndose $\sqcup$, $\sqcap$ y $'$ como operaciones derivadas.[52, 53]

Observación 3.7.0.— En algunos textos suelen aparecer también en la definición de retículo las idempotencias $x \sqcup x = x$ y $x \sqcap x = x$, sin embargo, no es necesario, ya que, en realidad, es posible deducirlas de las leyes anteriores, en particular de las simplificativas. En efecto, veamos, por ejemplo, cómo demostrar la primera. Sea $y = x \sqcup x$; entonces, $x \sqcap y = x \sqcap (x \sqcup x) = x$ [simplificativa de $\sqcap$ en $\sqcup$], de donde, $x \sqcup x = x \sqcup (x \sqcap y) = x$ [simplificativa de $\sqcup$ en $\sqcap$]. Demostraríamos la segunda de forma análoga.

§ 3.7.2 El álgebra de Boole de la lógica de juntores

La cuaterna $(\mathcal{F}_0; \wedge, \vee, \neg)$ tiene estructura de álgebra de Boole, que por su definición como retículo distributivo y complementado[54] —siendo $\wedge$, $\vee$ y $\neg$ las operaciones correspondientes $\sqcap$, $\sqcup$ y $'$ de la definición, respectivamente—, significa que $(\mathcal{F}_0, \wedge, \vee, \neg)$

0. es un retículo, o sea, satisface las propiedades

   - conmutativas[55] de $\vee$ y $\wedge$ en $\mathcal{F}_0$, esto es, para cualesquiera ϕ, ψ de $\mathcal{F}_0$ se satisface

$$\phi \vee \psi = \psi \vee \phi,$$
$$\phi \wedge \psi = \psi \wedge \phi,$$

   - asociativas[56] de $\vee$ y $\wedge$ en $\mathcal{F}_0$, esto es, para cualesquiera ϕ, ψ, χ de $\mathcal{F}_0$ se satisface

$$(\phi \vee \psi) \vee \chi = \phi \vee (\psi \vee \chi),$$
$$(\phi \wedge \psi) \wedge \chi = \phi \wedge (\psi \wedge \chi),$$

[52] *Vid.* https://writings.stephenwolfram.com/2018/11/logic-explainability-and-the-future-of-understanding/; en este artículo, Stephen Wolfram relata la evolución de las definiciones basadas en una única operación, desde la de tres axiomas de Henry Sheffer de 1913 hasta la suya de un axioma, pasando por las de Carew Meredith de dos axiomas de 1949 y 1967 y tres de 1969.

[53] *Vid.* https://writings.stephenwolfram.com/2025/01/who-can-understand-the-proof-a-window-on-formalized-mathematics/.

[54] *Vid. supra* definición 3.17 (pág. 354 de esta edición).

[55] *Cfr. supra* teorema 10.7.1 (pág. 544 de esta edición) y teorema 10.9.1 (pág. 545 de esta edición), respectivamente.

[56] *Cfr. supra* teorema 10.7.2 (pág. 544 de esta edición) y teorema 10.9.2 (pág. 545 de esta edición), respectivamente.

- simplificativas[57], de $\vee$ respecto de $\wedge$ y de $\wedge$ respecto de $\vee$, esto es, para cualesquiera ϕ, ψ de $\mathcal{F}_0$ se satisface

$$\phi \vee (\psi \wedge \phi) = \phi,$$
$$\phi \wedge (\psi \vee \phi) = \phi;$$

1. es un retículo distributivo, esto es, satisface además las propiedades

- distributivas[58], de $\vee$ respecto de $\wedge$ y de $\wedge$ respecto de $\vee$, esto es, para cualesquiera ϕ, ψ, χ de $\mathcal{F}_0$ se satisface

$$\phi \vee (\psi \wedge \chi) = (\phi \vee \psi) \wedge (\phi \cup \chi),$$
$$\phi \wedge (\psi \vee \chi) = (\phi \wedge \psi) \vee (\phi \wedge \chi);$$

2. es un retículo distributivo y complementado, o sea, satisface además que

- es acotado, esto es, que existen los elementos neutros[59] de $\vee$ y $\wedge$ en $\mathcal{F}_0$, esto es, para todo ϕ de $\mathfrak{F}$ se satisface

$$\phi \vee 0 = \phi,$$
$$\phi \wedge 1 = \phi,$$

- se satisfacen las leyes de complementación[60] para $\vee$ y $\wedge$ en $\mathcal{F}_0$, esto es, para todo ϕ de $\mathcal{F}_0$ se satisface

$$\phi \vee \neg\phi = 1,$$
$$\phi \wedge \neg\phi = 0.$$

§ 3.8 Cuatro facetas de la semántica

Aunque estas cuatro facetas de la semántica se exploran y utilizan profusamente a la hora de definir un lenguaje de programación —en el marco de la *teoría de dominios*—, no está de más proporcionar unas ligeras pinceladas en el contexto presente.

Dependiendo del grado de abstracción y de la meta a conseguir, se distingue entre la semántica operacional, la semántica denotacional, la semántica algebraica y la semántica axiomática.

[57] *Cfr. supra* teorema 10.10.0 (pág. 545 de esta edición) y teorema 10.10.1 (pág. 545 de esta edición), respectivamente.
[58] *Cfr. supra* teorema 10.10.2 (pág. 545 de esta edición) y teorema 10.10.3 (pág. 545 de esta edición), respectivamente.
[59] *Cfr. supra* teorema 10.7.3 (pág. 544 de esta edición) y teorema 10.9.3 (pág. 545 de esta edición), respectivamente.
[60] *Cfr. supra* teorema 10.14.0 (pág. 549 de esta edición) y teorema 10.14.1 (pág. 549 de esta edición), respectivamente.

§ 3.8.0 Semántica operacional

Definición 3.20.— Una *semántica operacional* (o, sinónimamente, *semántica intensional* o *semántica de paso pequeño*) es un *sistema de reescritura de términos* más un conjunto de reglas de inferencia, llamadas *reglas de reescritura*, que establece de forma precisa cómo se produce un paso del cálculo.

En el contexto de los lenguajes de programación esta semántica se centra en cómo se obtiene el resultado de un programa en una máquina abstracta concreta o genérica.

En una semántica operacional el significado de una expresión sintáctica (una fórmula en el caso de la lógica) es la traza de los pasos de su procesamiento de acuerdo a unas reglas establecidas. Por ejemplo, dos fórmulas distintas y cuyas FND sean la misma, tienen diferente significado respecto de la misma semántica operacional, ya que sus trazas serían las correspondientes secuencias de los respectivos pasos de sus correspondientes procesos de transformación en FND. Es habitual decir que tienen diferentes semánticas operacionales.

Ejemplo 175

Definir una semántica operacional para el cálculo lógico conjuntivo de izquierda a derecha y obtener los significados de $(0 \wedge 1) \wedge (1 \wedge 1)$ y $1 \wedge (0 \wedge 1)$.

Resolución.— Por un momento, pensemos en los valores de verdad como números 0 y 1 y en $\wedge$ como el producto aritmético de naturales —en realidad, basta que lo consideremos en $\{0,1\}$—. Para la aritmética del producto hay sólo una regla de reescritura, a saber, $n' \cdot n'' \vdash n$, donde n es el producto de los números n' y n''; en otras palabras, el producto de dos números es un paso de cálculo. Pensemos ahora en $\{0,1\}$, en el operador $\wedge$ y en un cálculo arbitrario; la equivalente a la regla anterior es $n' \wedge n'' \vdash n$, con $n = [n' \wedge n'']$, es decir, n es el valor de verdad ($n \in \{0,1\}$) de la operación $\wedge$ actuando sobre dos valores de verdad ($n', n'' \in \{0,1\}$).

Se proponen las reglas siguientes para producir el cálculo conjuntivo de izquierda a derecha.

$$R_0 : \frac{\phi \vdash \phi'}{\phi \wedge \psi \vdash \phi' \wedge \psi} \quad R_1 : \frac{\psi \vdash \psi'}{n \wedge \psi \vdash n \wedge \psi'} \quad R_2 : n' \wedge n'' \vdash n \; (n \text{ es } [n' \wedge n''])$$

Obtención del significado de $(0 \wedge 1) \wedge (1 \wedge 1)$.

Por R_0,

$$\frac{0 \wedge 1 \vdash 0}{(0 \wedge 1) \wedge (1 \wedge 1) \vdash 0 \wedge (1 \wedge 1)},$$

ahora, por R_1,

$$\frac{(1 \wedge 1) \vdash 1}{0 \wedge (1 \wedge 1) \vdash 0 \wedge 1},$$

finalmente, por R_2,

$$0 \wedge 1 \vdash 0 \text{ (pues 0 es } [0 \wedge 1]);$$

el significado de $(0 \wedge 1) \wedge (1 \wedge 1)$ es su traza, esto es, la secuencia de los estados de computación hasta obtener la respuesta 0, es decir, $\langle (0 \wedge 1) \wedge (1 \wedge 1), 0 \wedge (1 \wedge 1), 0 \wedge 1 \rangle$.

Obtención del significado de $1 \wedge (0 \wedge 1)$.

Por R_1,

$$\frac{(0 \wedge 1) \vdash 0}{1 \wedge (0 \wedge 1) \vdash 1 \wedge 0},$$

ahora, por R_2,

$$1 \wedge 0 \vdash 0 \text{ (pues 0 es } [1 \wedge 0]);$$

el significado de $1 \wedge (0 \wedge 1)$ es su traza, esto es, la secuencia de los estados de computación hasta obtener la respuesta 0, es decir, $\langle 1 \wedge (0 \wedge 1), 1 \wedge 0 \rangle$. ■

§ 3.8.1 Semántica denotacional

En una `semántica denotacional` (o, sinónimamente, *semántica extensional*) se asigna un significado matemático a la sintaxis, esto es, el significado de una fórmula es una función matemática, una relación.

En el contexto de los lenguajes de programación esta semántica se centra en la función que computa un programa, en qué hace el programa sin ocuparse del cómo lo hace.

Por ejemplo, dos fórmulas distintas y lógicamente equivalentes tienen la misma semántica denotacional. Esto es así por lo siguiente: sean dos fórmulas distintas, ϕ y ψ, ambas equivalentes lógicamente y, por tanto, equivalentes a una tercera, $\phi \equiv \chi$ y $\psi \equiv \chi$; en este caso, lo realmente importante es que la relación entre ϕ y χ es la misma que entre ψ y χ, esto es, igual pasaría si, por ejemplo, en vez de una relación de equivalencia lógica ($\equiv$) fuese de consecuencia lógica ($\models$).

Ejemplo 176

La semántica denotacional de la conjunción (considerando 0 y 1 fórmulas, a saber, $\bot$ y $\top$, respectivamente) es

$$\begin{array}{rccl} Y: & F & \longrightarrow & \{0,1\} \\ & n & \longmapsto & Y(n) = n \\ & \phi \wedge \psi & \longmapsto & Y(\phi \wedge \psi) = y(Y(\phi), Y(\psi)), \end{array}$$

donde $n \in \{0,1\}$ e y es la función diádica $y : \{0,1\} \times \{0,1\} \to \{0,1\}$ que asocia a cada par de dígitos binarios su composición conjuntiva. Hallemos la semántica denotacional de $(0 \wedge 1) \wedge (1 \wedge 1)$.

Resolución.— Según la definición dada, la semántica denotacional de $(0 \wedge 1) \wedge (1 \wedge 1)$ es

$$\begin{aligned} Y((0 \wedge 1) \wedge (1 \wedge 1)) &= y(Y(0 \wedge 1), Y(1 \wedge 1)) \\ &= y(y(Y(0), Y(1)), y(Y(1), Y(1))) \\ &= y(y(0,1), y(1,1)) \\ &= y(0,1) \\ &= 0, \end{aligned}$$

que, por cierto, nos informa de que la razón por la cual el significado de $(0 \wedge 1) \wedge (1 \wedge 1)$ es 0 es porque el significado de $0 \wedge 1$ es 0 y el de $1 \wedge 1$ es 1. ■

En definitiva, la semántica denotacional establece el significado de una fórmula en función de los significados de sus subfórmulas.

§ 3.8.2 Semántica algebraica

En el contexto de los lenguajes de programación, la `semántica algebraica` se centra en proveer de ecuaciones, inecuaciones y estructuras para comparar, transformar y optimizar diseños y programas.

Ejemplo 177

La semántica algebraica de la conjunción viene dada por el álgebra de Boole de la lógica de juntores. Hallemos la semántica algebraica de $(0 \wedge 1) \wedge (1 \wedge 1)$.

Resolución.— Según el álgebra de Boole de la lógica de juntores, la semántica algebraica de $(0 \wedge 1) \wedge (1 \wedge 1)$ es

$$\begin{aligned} 0 \wedge 1 \wedge 1 \wedge 1 &= 0 \wedge (1 \wedge (1 \wedge 1)) && \text{(asociatividad de } \wedge) \\ &= 0 \wedge (1 \wedge 1) && \text{(idempotencia de 1)} \\ &= 0 \wedge 1 && \text{(idempotencia de 1)} \\ &= 0; && \text{(dominancia de 0)} \end{aligned}$$

en definitiva, el significado de $(0 \wedge 1) \wedge (1 \wedge 1)$ es 0. ■

Aunque pudiese parecer que al igual que la semántica denotacional, la semántica algebraica establece el significado a partir del significado de las subfórmulas, lo cierto es que el proceso intermedio es puramente sintáctico, y obedece a las reglas de la estructura, en este caso, un álgebra de Boole, es decir, es un cálculo interno a la estructura; en otras palabras, el significado se obtiene como interpretación del resultado de dicho cálculo.

§ 3.8.3 Semántica axiomática

En una semántica axiomática, el significado de una fórmula viene dado por una proposición lógica. Por ejemplo, $p \vee \neg p$ y $\neg(\neg p \wedge p)$ son dos semánticas axiomáticas de la tautología $\top$. La semántica axiomática es adecuada para investigar propiedades directamente.

Ejemplo 178

Demostremos que $(0 \wedge 1) \wedge (1 \wedge 1)$: es-una-entidad-artificial —es decir, que satisface esta propiedad— en la semántica axiomática definida por:

0. n: es-una-entidad-artificial si, y sólo si, $n = 0$;
1. n: es-una-entidad-natural si, y sólo si, $n = 1$;
2. $$\frac{\phi\colon P \qquad \psi\colon Q}{\phi \wedge \psi\colon R}$$ donde $R =$ es-una-entidad-natural si, y sólo si, $P = Q =$ es-una-entidad-natural.

Resolución.— En efecto, así es según la derivación

$$\cfrac{\cfrac{0\colon \text{es-una-entidad-artificial} \qquad 1\colon \text{es-una-entidad-natural}}{0 \wedge 1\colon \text{es-una-entidad-artificial}} \qquad \cfrac{1\colon \text{es-una-entidad-natural} \qquad 1\colon \text{es-una-entidad-natural}}{1 \wedge 1\colon \text{es-una-entidad-natural}}}{(0 \wedge 1) \wedge (1 \wedge 1)\colon \text{es-una-entidad-artificial}}$$



Observación 3.8.0.— En el caso de la semántica denotacional, de interesarnos demostrar una propiedad para un conjunto de fórmulas, la estrategia estándar de demostración sea la inducción estructural, mientras que en la semántica operacional, para demostrar una propiedad para la semántica definida pudiésemos utilizar la inducción débil o fuerte; aunque estudiaremos estos tres tipos de inducción, entre otros, en § 16 (pág. 804 de esta edición), su aplicación en la semántica supera los objetivos de estas notas[61].

[61] *Cfr. v. gr.* Nielson y Nielson [95]).

§ 3.9 Bibliografía

- Para la semántica de la lógica de juntores, en general:
  - Para una primera aproximación:

[62] María MANZANO ARJONA y Antonia HUERTAS SÁNCHEZ. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

[63] Pascual CASAÑ MUÑOZ y Amador ANTÓN ANTÓN. *Lógica matemática. Ejercicios. I. Lógica de enunciados*. NAU llibres, Valencia, España, 1991.

  - Para estudiar, practicar y conocer más:

[64] Manuel GARRIDO GIMÉNEZ. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

[65] Carmen GARCÍA TREVIJANO. *El arte de la lógica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1999.

  - Para profundizar, acullá:

[66] Manuel GARRIDO GIMÉNEZ, Luis Manuel VALDÉS VILLANUEVA, Jesús MOSTERÍN DE LAS HERAS, Alfonso GARCÍA SUÁREZ y Carlos-Peregrín FERNÁNDEZ OTERO. *Lógica y lenguaje*. Cuadernos de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1989.

[67] Raymond Merrill SMULLYAN. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

[60] Herbert Bruce ENDERTON. *A mathematical introduction to logic*. Harcourt/Academic Press, San Diego, Condado de San Diego, California (US-CA), Estados Unidos de América, 2.ª ed., 2001.

- Para el caso particular de las tablas analíticas/semánticas (TA/S) en la lógica de juntores:
  - Para una primera aproximación:

[62] María MANZANO ARJONA y Antonia HUERTAS SÁNCHEZ. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

[63] Pascual CASAÑ MUÑOZ y Amador ANTÓN ANTÓN. *Lógica matemática. Ejercicios. I. Lógica de enunciados*. NAU llibres, Valencia, España, 1991.

- Para estudiar, practicar y conocer más:

[64] Manuel Garrido Giménez. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

- Para profundizar, acullá:

[67] Raymond Merrill Smullyan. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

[90] Evert Willem Beth. *The Foundations of Mathematics. A Study in the Philosophy of Science*. North-Holland, Amsterdam, Países Bajos, 1959.

[91] Kaarlo Jaakko Juhani Hintikka. *The Philosophy of Mathematics*. Oxford, 1969.

[96] Rafael Beneyto Torres. Laberintos analíticos. *Teorema: Revista internacional de filosofía*, 1(4):19–30, 1971.

[97] Kaarlo Jaakko Juhani Hintikka. Form and content in quantification theory. *Acta Philosophica Finnica*, 8:57–55, 1955.

[98] Richard Carl Jeffrey. *Formal Logic: its Scope and Limits*. McGraw-Hill, 1967.

Capítulo 4

De la lógica de primer orden

—Pondré un examen parcial sorpresa de aquí a final de curso.
María piensa: no puede ser el último día, porque no sería sorpresa; tampoco puede ser el penúltimo, porque si no ha sido el antepenúltimo, como no puede ser el último, sabríamos que sería el penúltimo; y así sucesivamente, hasta mañana; en fin, que no puede poner un examen sorpresa ningún día de los que dice.
Pasaron unos días.
—Hola, ¡vamos con el examen que os dije!
—Pero usted no puede poner el examen —dice María y le cuenta su argumentación.
—Pues el hecho es que como no te lo esperabas, el examen de hoy es toda una sorpresa para ti (y para los demás), ¿verdad?

(Acervo popular).

Profundizamos en el análisis de las afirmaciones, pudiendo ahora distinguir ciertas cuantificaciones, esto es, pudiendo decir en algún sentido el número de entidades de una colectividad que satisfacen ciertas propiedades o relaciones.

§ 4.0 El lenguaje $\mathcal{L}_1$ de la lógica de primer orden

§ 4.0.0 Variable funtorial, función lógica y función de verdad

Si bien las funciones son un caso particular de relaciones, la costumbre moderna en matemática de separar su estudio nos lleva a hacerlo igualmente en lógica. De aquí que integremos explícitamente las *variables funtoriales* como parte esencial del vocabulario de la lógica de primer orden. Un ejemplo de variable funtorial es $f \leftrightharpoons$ Cónyuge de , esto es, $fx \leftrightharpoons$ Cónyuge de x, por lo que si a y b son cónyuges, $fa = b$ y $fb = a$. Un caso particular de variable funtorial es la *función lógica*, cuando sus argumentos son entidades pero su valor es un valor lógico; por ejemplo, $gxy \leftrightharpoons x$ e y son cónyuges, por lo que si a y b son cónyuges, $gab = gba = 1$. Otro caso particular es el de *función de verdad*, una función valorada en $\{0,1\}$ con argumentos variables proposicionales. Una fórmula de la lógica de juntores lo es; a modo de ejemplo, la función $(p \vee q) : \{\langle 1,1\rangle, \langle 1,0\rangle, \langle 0,1\rangle, \langle 0,0\rangle\} \longrightarrow \{0,1\}$ definida por $(p \vee q)(1,1) = 1$, $(p \vee q)(1,0) = 1$, $(p \vee q)(0,1) = 1$ y $(p \vee q)(0,0) = 0$.

§ 4.0.1 El vocabulario

El lenguaje de la lógica de cuantores incluye el lenguaje de la lógica de juntores.

Definición 4.0.— Definimos el lenguaje $\mathcal{L}_1$ de la lógica de primer orden mediante un alfabeto compuesto por:

0. la colección finita $\mathcal{J}$ de *juntores* de la lógica de juntores, medádicos, $\bot$ y $\top$, monádicos, id y $\neg$, y diádicos, $\bot$, id_0, id_1, $\neg_0$, $\neg_1$, $\vee$, $\wedge$, $\veebar$, $\rightarrow$, $\leftarrow$, $\nrightarrow$, $\nleftarrow$, $\leftrightarrow$, $|$, $\downarrow$ y $\top$;

1. una colección finita $\mathcal{Q}$ de *cuantores* (signos lógicos de cuantificación de las variables de sujeto), $\top$, $\overline{\forall}$, $\overline{\exists^\circ}$, $\overline{\exists}$, $\exists$, $\exists^\circ$, $\forall$, $\bot$, según la notación que estableceremos más adelante, habiendo, como veremos, un total de ocho;

2. una colección infinita numerable $\mathcal{C}$ de *signos no lógicos de constantes de sujeto*, que representan entidades concretas del universo: $a, b, c, \ldots$, ocasionalmente anotadas con subíndices, $a_0, b_0, c_0, \ldots, a_k, b_k, c_k, \ldots$;

3. una colección infinita numerable $\mathcal{X}$ de *signos no lógicos de variables de sujeto* —o *subjetivas*—, que representan entidades arbitrarias del universo: $x, y, z, \ldots$, ocasionalmente anotadas con subíndices, $x_0, y_0, z_0, \ldots, x_k, y_k, z_k, \ldots$;

4. la colección infinita numerable $\mathcal{V}$ de *letras/signos/variables enunciativas/proposicionales* de la lógica de juntores, que representan proposiciones simples: $p, q, r, \ldots$, ocasionalmente anotadas con subíndices, $p_0, q_0, r_0, \ldots, p_k, q_k, r_k, \ldots$;

5. una colección infinita numerable $\mathcal{P}$ de *letras/signos/variables predicativas*, que representan predicados, esto es, propiedades, relaciones: $P, Q, R, \ldots$, ocasionalmente anotadas con subíndices, $P_0, Q_0, R_0, \ldots$, y, a veces, con un superíndice indicador de su aridad, $P_k^n, Q_k^n, R_k^n, \ldots$;

6. una colección infinita numerable $\mathcal{F}_u$ de *letras/signos/variables funtoriales*, que representan funciones: $f, g, h, \ldots$, ocasionalmente anotadas con subíndices, $f_0, g_0, h_0, \ldots$, y, a veces, con un superíndice indicador de su aridad, $f_k^n, g_k^n, h_k^n, \ldots$;

7. el *signo de verdad*, 1 (o V), y el *signo de falsedad*, 0 (o F);

8. una colección finita de signos ortográficos[∘], de puntuación y auxiliares, con funciones organizativas, de delimitación, determinación o aclaración, entre otras; algunos ejemplos son: () (paréntesis —redondos—), [] (corchetes —paréntesis cuadrados]), {} (llaves —paréntesis aquillados o aballestados—), ⟨⟩ (corchetes angulares), etc.

9. la colección infinita numerable de letras latinas mayúsculas $A, B, C, \ldots$, ocasionalmente anotadas con subíndices, $A_0, A_1, \ldots$, de *variables semánticas*, que representan proposiciones, simples y compuestas de la lógica de juntores, y cuantificadas de la lógica de cuantores;

10. la colección infinita numerable de letras griegas minúsculas, $\phi, \psi, \chi, \tau, \ldots$, ocasionalmente anotadas con subíndices, $\phi_0, \phi_1, \ldots$, de *variables sintácticas*, que representan las fórmulas, y

11. la colección infinita numerable de letras griegas mayúsculas, $\Gamma, \Delta, \Phi, \Psi, \ldots$, ocasionalmente anotadas con subíndices, $\Phi_0, \Phi_1, \ldots$, que representan colecciones de fórmulas.

§ 4.0.2 La fórmula

Al igual que en lógica de juntores, es posible definir inductivamente una fórmula.

Definición 4.1.— Un *término*[1] es:

0. una constante de sujeto, o

1. una variable funtorial enádica seguida de n términos, con $n \geq 1$.

Definición 4.2.— Dada una base de juntores, una *fórmula bien formada* o, simplemente, *fórmula*, de la lógica de primer orden es toda fila de signos que satisfaga alguna de las siguientes condiciones:

0. toda variable proposicional y toda variable predicativa enádica seguida de n términos son fórmulas, que llamaremos *fórmulas atómicas*;

1. una fórmula precedida del juntor $\neg$ es una fórmula;

∘ *Cfr. v. gr.* https://www.rae.es/dpd/signos ortográficos.

1 Son términos las constantes $a, b, c, \ldots$, las funciones de términos, $fa, gab, hgabfcd, \ldots$ En algunos textos aparece el que hemos definido como *término básico* con la finalidad de diferenciarlo del «término» que incluyese variables; en otros textos, a este último se le denomina *término complejo*.

2. una fórmula seguida de un juntor de la base de juntores, distinto de $\neg$, seguida de una fórmula, y habiendo hecho buen uso de los paréntesis, es una fórmula;

3. si x es una variable subjetiva y ϕ es una fórmula, ϕ^a_x es la fórmula resultante de la sustitución en ϕ de la constante individual a por x y $C = \{\exists, \forall\} \subseteq \mathcal{Q}$, entonces $\forall x \phi^a_x$ y $\exists x \phi^a_x$ son fórmulas.

Únicamente las fórmulas obtenidas aplicando 0, 1, 2 o 3, son fórmulas.

Observación 4.0.0.— La sustitución en una fórmula ϕ de una letra a por otra, digamos $\sigma(a)$, suele notarse $\phi\left(\substack{a\\ \sigma(a)}\right)$. Esta notación proviene de las sustituciones[2]. Nosotros, aquí, en el ámbito de la lógica, relajamos la notación quitando los paréntesis, incluso a σ por ser una letra funtorial: $\phi^a_{\sigma a}$. Similarmente si lo que sustituimos es una variable.

Observación 4.0.1.— Este es el punto de vista de la lógica tradicional. Actualmente, se entiende por *sujeto* cualquier nombre propio y por *predicado* cualquier nombre común. Así, si consideramos la expresión «María es agradable», las terminologías tradicional y actual coinciden: «María» es el sujeto y «agradable» el predicado: Pa —donde $Px \leftrightharpoons$ x es agradable y $a \leftrightharpoons$ María—; sin embargo, en «toda mujer es agradable», según la terminología tradicional, «mujer» es el sujeto y «agradable» el predicado, pero según la actual, ambos son predicados: $\forall x(Mx \to Ax)$ —donde $Mx \leftrightharpoons$ x es mujer—.

Observación 4.0.2.— También pudiésemos notar de manera nemotécnica los predicados y sujetos, así tendríamos, por ejemplo,

- Agradable(María);
- Carácter(María, agradable);
- Carácter(Mujer(x), Agradable(x));
- $\forall x$ (Mujer(x) $\to$ Agradable(x)).

Observación 4.0.3.— Es posible sustituir el conjunto C de la definición de fórmula por cualquier base de cuantores[3].

Definición 4.3.— Llamamos *subfórmula* a cualquier parte de una fórmula que sea a su vez una fórmula.

[2] *Cfr. infra* § 17.5.6 (pág. 870 de esta edición).
[3] *Cfr. infra* § 4.1.7 (pág. 380 de esta edición).

Ejemplo 179

Proporcionemos ejemplos de términos, fórmulas atómicas, fórmulas y subfórmulas.

Resolución.—

0. Las expresiones a, b, fa, gab, h^3faab son términos;
1. las expresiones p, q, Pa, Qab, R^3g^2abbc son fórmulas atómicas;
2. las expresiones $p \wedge \neg q$, $\neg\forall x Px$, $\exists x \neg Px$ y $\forall x \exists y Qxy$ son fórmulas;
3. $\neg q$ es una subfórmula de $p \wedge \neg q$ y ésta de $q \vee (p \wedge \neg q) \rightarrow \neg p$. ■

§ 4.0.3 Precedencia de cuantores y juntores

Salvo que los signos de puntuación indiquen otra cosa, los cuantores son menos potentes que los juntores de la lógica de juntores.

Definición 4.4.— *Grado lógico* de una fórmula de la lógica de primer orden es el número de juntores y cuantores que posee, contando las repeticiones.

Ejemplo 180

Hallemos el grado lógico de las siguientes fórmulas:

0. $\forall x\, (\neg Px \rightarrow Qx)$;
1. $\exists x\, (Qx \wedge \neg\forall y Qy) \rightarrow \forall x Rx$.

Resolución.—

0. Grado_Lógico[$\forall x\, (\neg Px \rightarrow Qx)$] $= 3$, ya que tiene dos juntores ($\neg$ y $\rightarrow$) y un cuantor ($\forall$);
1. Grado_Lógico[$\exists x\, (Qx \wedge \neg\forall y Qy) \rightarrow \forall x Rx$] $= 6$, ya que tiene tres juntores ($\wedge$, $\neg$ y $\rightarrow$) y tres cuantores ($\exists$, $\forall$ y $\forall$). ■

Definición 4.5.— Llamamos *signo dominante* de una fórmula de la lógica de primer orden al signo lógico más potente. El uso correcto de paréntesis es esencial a la hora de determinar cuál es el signo lógico más potente.

Ejemplo 181

Hallemos el signo dominante de las siguientes fórmulas:

0. $\forall x\,(\neg Px \to Qx)$;
1. $\exists x\,(Qx \wedge \neg\forall y Qy) \to \forall x Rx$.

Resolución.—

0. Signo_Dominante$[\forall x\,(\neg Px \to Qx)] = \forall$;
1. Signo_Dominante$[\exists x\,(Qx \wedge \neg\forall y Qy) \to \forall x Rx] = \to$. ■

Definición 4.6.— Llamamos *alcance* de un signo lógico en una fórmula de la lógica de primer orden al conjunto de fórmulas o subfórmulas del que sea signo dominante. Similarmente a lo que sucede para el signo dominante, el uso correcto de paréntesis es esencial a la hora de determinar el alcance de un signo lógico.

Ejemplo 182

Sean $A \risingdotseq \forall x\,(\neg Px \to Qx)$ y $B \risingdotseq \forall x\,(\exists y\,(Pxy \wedge Qxy) \to Rx)$. ¿Cuál es el alcance de $\to$ en A, de $\exists y$ en B y de $\forall x$ en B?

Resolución.— Son los siguientes:

- Alcance$[\to; A] = \{\neg Px, Qx\}$;
- Alcance$[\exists y; B] = \{Pxy \wedge Qxy\}$;
- Alcance$[\forall x; B] = \{\exists y\,(Pxy \wedge Qxy) \to Rx\}$. ■

Definición 4.7.— A las variables que están en el alcance de algún cuantor, las llamamos *ligadas* (o, sinónimamente, *aparentes*).

Definición 4.8.— A las variables que no caen dentro del alcance de ningún cuantor, las llamamos, precisamente, *libres* (o, sinónimamente, *reales*).

Definición 4.9.— Cuando una fórmula no contiene variables libres, esto es, cuando todas las variables de la fórmula están cuantificadas, o sea, están en el alcance de algún cuantor, decimos de la fórmula que es una *fórmula cerrada*; caso contrario, decimos que es una *fórmula abierta* —que también llamamos *pseudofórmula*—.

Ejemplo 183

¿Qué tipo de fórmulas son las expresiones $\forall x Px$, $\forall x \exists y Qxy$, Px y $\forall x Qxy$?

Resolución.— Las expresiones $\forall x Px$ y $\forall x \exists y Qxy$ son fórmulas cerradas; las expresiones Px y $\forall x Qxy$ son pseudofórmulas (fórmulas abiertas). ■

Salvo en cuestiones muy concretas, en estas notas no trabajaremos con fórmulas abiertas.

Observación 4.0.4.— En algunos textos, a las fórmulas abiertas se las denomina *predicados compuestos* y a las cerradas, *sentencias*.

Definición 4.10.— Un cuantor siempre va indizado por una o varias variables de sujeto. Llamamos *prefijo cuantorial* a esta yuxtaposición. Llamamos *matriz cuantorial* a la fórmula o subfórmula alcanzada por el prefijo.

Ejemplo 184

¿Cuántos y cuáles son los prefijos cuantoriales de B del ejemplo 182 (pág. 369 de esta edición)? ¿Cuáles son sus matrices cuantoriales respectivas?

Resolución.— Tenemos dos prefijos cuantoriales: $\forall x$ y $\exists y$, cuyas matrices son, respectivamente, $[\exists y\,(Pxy \land Qxy) \to Rx]$ y $[Pxy \land Qxy]$. ■

§ 4.1 Semántica para $\mathcal{L}_1$

§ 4.1.0 Cuantores

Definición 4.11.— Llamamos *cuantor* (o, sinónimamente, *cuantificador*) a toda expresión que nos diga, en algún sentido, cuántas entidades x satisfacen una cierta propiedad P.

Definición 4.12.— El *generalizador*, también llamado *cuantor universal*, que notamos $\forall$, designa el significado de «para todo». Expresándolo junto a una propiedad de x, lo simbolizamos $\forall x Px$, significando y leyéndose «toda entidad x satisface la propiedad P».

Definición 4.13.— El *particularizador*, también llamado *cuantor existencial*, que notamos $\exists$, designa el significado de «para algún». Expresándolo junto a una propiedad de x, lo simbolizamos $\exists x Px$, significando y leyéndose «alguna entidad x satisface la propiedad P».

Definición 4.14.— Llamamos predicado *monádico* al que afecta a un solo sujeto; *diádico* (o, sinónimamente, *binario*) si afecta a dos sujetos; y en general, *enádico* (o, sinónimamente, *n-ádico*) si afecta a n sujetos. Si el número de sujetos es indeterminado, hablamos de *predicado poliádico*.

Observación 4.1.0.— A los predicados monádicos también se les conoce como *propiedades* y a los diádicos y poliádicos como *relaciones*.

Ejemplo 185

Formalicemos los siguientes enunciados:

0. No todo el mundo sabe programar.
1. Algunos mamíferos nadan.
2. Existe un número entero que es mayor que cualquier otro.

[Cubit 36].

Resolución.— Los siguientes son ejemplos de sus formalizaciones.

0. Sean $Hx \leftrightharpoons x$ es ser humano y $Px \leftrightharpoons x$ sabe programar, entonces la formalización del enunciado es $\neg\forall x(Hx \to Px)$.

1. Sean $Mx \leftrightharpoons x$ es mamífero y $Nx \leftrightharpoons x$ nada, entonces la formalización del enunciado es $\exists x(Mx \wedge Nx)$.

2. Sean $Zx \leftrightharpoons x$ es entero y $Mxy \leftrightharpoons x$ es mayor o igual que y, entonces la formalización del enunciado es $\exists x(Zx \wedge \forall y(Zy \to Mxy))$. ■

Ejemplo 186

Formalicemos los siguientes enunciados:

0. Todo A que sea B, también es C.
1. Si cualquier A es B, entonces también es C.
2. No hay nada que sea A o B y no sea C.

[Cubit 37].

Resolución.— Los siguientes son ejemplos de sus formalizaciones.

0. $(\forall x)((Ax \wedge Bx) \to Cx)$.

1. Puede reescribirse como «si cualquier A es B, entonces también cualquier A es C», por tanto, $(\forall x(Ax \to Bx)) \to (\forall x(Ax \to Cx))$.

¡Cuidado!: si $\forall x(Px \rightarrow Qx)$, entonces $(\forall x Px) \rightarrow (\forall x Qx)$, pero $(\forall x Px) \rightarrow (\forall x Qx)$ no implica que $\forall x(Px \rightarrow Qx)$.

2. $(\neg\exists x)((Ax \vee Bx) \wedge \neg Cx)$. O con otras palabras, «si algo es A o B entonces es C», esto es, $(\forall x)((Ax \vee Bx) \rightarrow Cx)$. ■

Ejemplo 187

Formalicemos los enunciados:

0. Las variables de programa x e y no son alias (esto es, nunca referencian la misma ubicación de memoria al mismo tiempo).
1. La variable x referencia una celda de memoria que tiene un autociclo.
2. Dos o más celdas de memoria apuntan a la celda m_0.

Resolución.— Los siguientes son ejemplos de sus formalizaciones, siendo $R(x, y)$ el predicado la variable o celda x apunta a la celda y:

0. $(\forall m)\neg(R(x, m) \wedge R(y, m))$.

1. $(\exists m)(R(x, m) \wedge R(m, m))$.

2. $(\exists m, m')(R(m, m_0) \wedge R(m', m_0) \wedge m \neq m')$. ■

Observación 4.1.1.— Los cuantores son representados de diversas formas en los textos. Nuestra terminología es la de Gentzen y Kleene. Hay quienes simbolizan los cuantores universal y existencial en la forma $\bigwedge$ y $\bigvee$, respectivamente. También quienes lo hacen en la forma Π y Σ, respectivamente. Y también quienes usan paréntesis en la forma $(\forall x P(x))$, representando un predicado poliádico por $P(x_1, x_2, \ldots, x_n)$ en vez de $Px_1x_2 \ldots x_n$.

Al hablar de lógica de primer orden queremos decir que admitimos tan sólo la cuantificación de las variables subjetivas. Esto es, no consideramos expresiones del tipo $\forall P Px$, que se sitúan en la denominada *lógica de segundo orden* —también conocida como *lógica superior*—.

Imaginemos que quisiéramos formalizar la expresión «todo el mundo tiene algo». Pudiésemos formalizar «x tiene y» por Txy; entonces se cuantificaría así: $\forall x\exists y Txy$, representando esto la expresión «todo el mundo tiene algo». Cuando, como aquí, se trata de predicados con más de una variable, hablaremos de *cuantificación poliádica*. En ella, debemos tener cuidado al utilizar los cuantores: siguiendo el ejemplo anterior, $\exists y\forall x Txy$ significa «hay algo que tiene todo el mundo», que no es, obviamente, lo que deseábamos formalizar.

Ejemplo 188

Formalicemos «hay una tortuga que corre más que todos los gatos y todos los perros».

Resolución.— Pudiésemos formalizar «x corre más que y» por Cxy; entonces $\exists x \forall y \forall z(Cxy \wedge Cxz)$ representa la expresión. ■

Es posible reescribir en un formato más compacto cualquier secuencia del mismo cuantor afectando a distintas variables; por ejemplo, reescribir $\exists x \forall y \forall z(Cxy \wedge Cxz)$ como $\exists x \forall_2 yz(Cxy \wedge Cxz)$ o, de manera más simple, $\exists x \forall yz(Cxy \wedge Cxz)$.

Definición 4.15.— En las expresiones también pueden aparecer *constantes*, esto es, entidades específicas del universo. Se representan con letras minúsculas, si bien de las primeras del alfabeto.

Ejemplo 189

Siendo $Mxy \leftrightharpoons x$ es mayor o igual que y, ¿es verdadera la expresión $\forall y May$ en el universo $\mathbb{Z}$ de los números enteros?

Resolución.— $\forall y May$ es falsa en el universo $\mathbb{Z}$ de los números enteros, pues no existe ningún número entero a mayor que todos los demás; sin embargo, es verdadera en el universo $\mathbb{Z}^-$ de los números enteros negativos, pues en este caso a es -1. ■

§ 4.1.1 Interpretación y modelo

Definición 4.16.— Una *interpretación* para una fórmula de la lógica de primer orden es un par (U, I), siendo:

0. U, una colección de entidades no vacía, que denominamos *universo* —que también llamaremos *ámbito/contexto/dominio/región/territorio* (*de discurso/de interpretación/de referencia*) o *referencial*—;
1. I, una función que asocia, a cada símbolo de constante, una entidad del universo, y a cada símbolo de predicado, una relación de la misma aridad sobre U.

Definición 4.17.— Un *modelo para una fórmula* es cualquier interpretación para la que dicha fórmula sea verdadera. Un *modelo para un conjunto de fórmulas* es cualquier interpretación para la que todas las fórmulas del conjunto sean verdaderas.

Ejemplo 190

Encontremos una interpretación para la fórmula $Pab \wedge \exists xyPxy$ —que abrevia $Pab \wedge (\exists x, y \in U)(Pxy)$— que no sea modelo para ella.

Resolución.— Con la interpretación $U = \{1, 2, 3\}$, $I(a) = 3$, $I(b) = 2$, $I(P) =<$ (es decir, $Pxy \fallingdotseq x < y$), dicha fórmula se expresa como la proposición $(3 < 2) \wedge (\exists x, y \in \{1, 2, 3\})(x < y)$, que es falsa por serlo $3 < 2$, y eso aunque $(\exists x, y \in \{1, 2, 3\})(x < y)$, ya que se trata de una conjunción. De aquí que podamos afirmar que dicha interpretación (U, I) no es un modelo para $Pab \wedge \exists xyPxy$. ■

Observación 4.1.2.— Recordemos que es posible utilizar alternativamente las notaciones Pxy o $P(x, y)$; por otro lado, si resulta claro del contexto con qué universo U trabajamos, entonces pudiésemos suprimirlo de la proposición. En el ejemplo 190 (pág. 374 de esta edición), pudiésemos reescribir $(3 < 2) \wedge (\exists x, y \in \{1, 2, 3\})(x < y)$ como $(3 < 2) \wedge \exists x, y(x < y)$. Notemos de paso que la eliminación de los paréntesis que circunscriben a $3 < 2$ pudiese generar ambigüedad; pensemos que $\exists x, y(x < y)$ fuese una fórmula insatisfactible o una fórmula válida, es decir, nítidamente 0 o 1, ¿estaríamos quizás preguntándonos si 3 es menor que 0 o 1? Mejor dejemos los paréntesis, ¿verdad?

Las fórmulas cerradas son proposiciones, las fórmulas abiertas, no. Notemos que Pa, donde a es un símbolo de constante, esto es, $a \in \mathcal{C}$, es una fórmula cerrada y, por tanto, es una proposición.

Ejemplo 191

Sean $A \fallingdotseq \forall x\,(\exists yPxy \wedge Qxy)$, $Pxy \fallingdotseq x \leq y$ y $Qxy \fallingdotseq y$ es múltiplo de x. Suponiendo que el dominio de interpretación es $\mathbb{Z}$, ¿es A una fórmula abierta o cerrada?

Resolución.— En tal interpretación, A no tiene un valor de verdad determinado, es una fórmula abierta. En efecto, dado un x, es posible elegir un y (por ejemplo, $y = 2x$) tal que $\exists yPxy$ sea verdadero, pero en Qxy, y puede tomar cualquier valor del dominio, independientemente del que haya tomado para verificar $\exists yPxy$. En este caso, para los valores de y que sean múltiplos de x, A es verdadera, mientras que para los y que no sean múltiplos de x, A es falsa. Esto se debe a que el único cuantor que alcanza a Qxy, $\forall$, sólo liga la variable x, dejando «libre» y. ■

Observación 4.1.3.— Ser un lenguaje de *primer orden* significa esencialmente dos cosas: por un lado, que el rango de las variables de sujeto sea el dominio, no más allá; por otro, que los cuantores cuantifiquen a las variables de sujeto y no, por ejemplo, a los predicados.

§ 4.1.2 Composición mediante cuantificación y su simbolización

Pensemos ahora en expresiones como:

A ≒ Todos los números naturales son mayores —en el sentido del orden habitual— o iguales que cero.

B ≒ Ningún número natural es negativo.

C ≒ Algún número natural es divisible por 2.

D ≒ Algún número natural no es divisible por 2.

E ≒ Existe un único número natural entre 22 y 24.

F ≒ Existe un único número natural que no es mayor que 1.

G ≒ Existe un número natural divisible por 2, pero no todos los números naturales son divisibles por 2 —o alternativamente: No todos los números naturales son divisibles por 2, aunque al menos uno sí lo es.

H ≒ Existe un número natural que no es primo, aunque no todos los números naturales son no primos —o alternativamente: No todos los números naturales son no primos, aunque al menos uno sí lo es (no primo).

I ≒ Para cualquier número primo, siempre puede encontrarse un número primo mayor —en el sentido del orden habitual— que él.

J ≒ Existe un número par que es simultáneamente igual a un primo más uno y a un primo menos uno.

Estos enunciados que también se consideran compuestos no son del tipo de los vistos hasta ahora, aunque en ellos puedan participar juntores. Se distinguen dos tipos básicos: universales y particulares.

Los enunciados universales se refieren a una afirmación o negación sobre todas las entidades de un sujeto plural, por ejemplo, los enunciados A y B anteriores, respectivamente, *universal afirmativo* y *universal negativo*. Un enunciado de este tipo es verdadero si, y sólo si, es verdadero cada enunciado resultante de la sustitución del sujeto plural por cada entidad. Por ejemplo, como son ciertas «$0 \geq 0$», «$1 \geq 0$», «$2 \geq 0$», y así sucesivamente, intuimos que «todos los números naturales son mayores o iguales que cero» es una proposición verdadera —que por otro lado es verdadera por definición del conjunto de números naturales—.

Los enunciados particulares se refieren a una afirmación o negación sobre un sujeto indeterminado, por ejemplo, los enunciados C y D anteriores, respectivamente, *particular afirmativo* y *particular negativo*. Un enunciado de este tipo es verdadero si, y sólo si, es verdadero al menos un enunciado resultante de la sustitución del sujeto indeterminado por alguna entidad. Por ejemplo, «algún número

natural es divisible por 2» es verdadero porque sustituyendo el sujeto indeterminado «algún número natural» por la entidad 2, el enunciado resultante «2 es divisible por 2» es verdadero.

Dos proposiciones particulares singulares son la *particularización única* —llamada también *particularización estricta*— y la *particularización no global* —llamada también *particularización fuerte*—.

La particularización única se refiere a una afirmación o negación de unicidad sobre un sujeto indeterminado, por ejemplo, los enunciados E y F anteriores, respectivamente, *particular de unicidad afirmativo* y *particular de unicidad negativo*. Un enunciado de este tipo es verdadero si, y sólo si, es verdadero un único enunciado de los resultantes de la sustitución del sujeto indeterminado por cada entidad. Por ejemplo, «existe un único número natural entre 22 y 24» es verdadero porque sustituyendo el sujeto indeterminado «un único número natural» por la entidad 23, el enunciado resultante «23 es el único número natural entre 22 y 24» es verdadero.

La particularización no global se refiere a una afirmación o negación de no globalidad sobre un doble sujeto indeterminado, por ejemplo, los enunciados G y H anteriores, respectivamente, *particular no global afirmativo* y *particular no global negativo*. Un enunciado de este tipo es verdadero si, y sólo si, es verdadero al menos uno pero no todos de los enunciados resultantes de la sustitución de los sujetos indeterminados por cada par de entidades. Por ejemplo, «existe un número natural divisible por 2, pero no todos los números naturales son divisibles por 2», que reescribimos «algún número natural es divisible por 2 y algún número natural es no divisible por 2» es verdadero porque sustituyendo los sujetos indeterminados «algún número natural» por la pareja de entidades 2 y 3, el enunciado resultante «2 es divisible por 2 y 3 no es divisible por 2» es verdadero.

Puede haber varias cuantificaciones en una misma expresión, por ejemplo, las proposiciones I y J anteriores.

§ 4.1.3 Simbolización de los cuantores

Siendo

$$Px \leftrightharpoons x \text{ es una de mis amistades,}$$
$$Qx \leftrightharpoons x \text{ dice siempre la verdad,}$$

veamos a continuación algunos de los símbolos que usaremos para designar los signos sentenciales cuantificativos, en particular, cómo se representan las proposiciones universales, particulares, particulares de unicidad y particulares fuertes:

- $\forall$ (*generalizador* o *cuantor universal*), por ejemplo, con los significados anteriores de Px y Qx, entonces $\forall x(Px \to Qx)$ representa «Todas mis amistades dicen siempre la verdad»;[4]

[4] Y tan cierto: «Leal es la herida que inflige el amigo, engañosa los besos del enemigo» (Proverbios 27, 6).

- $\exists$ (*particularizador* o *cuantor existencial*), por ejemplo, con los significados anteriores de Px y Qx, $\exists x(Px \wedge Qx)$ representa «Al menos una de mis amistades dice siempre la verdad»;
- $\exists!$ (*singularizador* o *cuantor existencial de unicidad*), por ejemplo, con los significados anteriores de Px y Qx, $\exists! x(Px \wedge Qx)$ representa «Sólo una de mis amistades dice siempre la verdad»[5]; también se nota por $\exists^1$;
- $\exists^\circ$ (*función cuantorial de existencia no global*), por ejemplo, con los significados anteriores de Px y Qx, $\exists^\circ x(Px \wedge Qx)$ representa «Al menos una de mis amistades dice siempre la verdad y al menos una de mis amistades no dice siempre la verdad»[6].

Observación 4.1.4.— He preferido utilizar «Al menos una de mis amistades» a «Alguna de mis amistades» o a «Algunas de mis amistades» por mor de la explicitud, pues pudiese parecer que «alguna» se refiriese a sólo una y «algunas» a necesariamente más de una.

Observación 4.1.5.— La negación de $\forall$ —notado en algunos textos por $\bigwedge$ o Π—, esto es, $\neg\forall$, se nota a veces por $\not\forall$ o por $\overline{\forall}$; la negación de $\exists$ —notado en algunos textos por $\bigvee$ o Σ—, esto es, $\neg\exists$, se nota a veces por $\nexists$ o por $\overline{\exists}$; la negación de $\exists!$, esto es, $\neg\exists$, se nota a veces por $\nexists!$ o por $\overline{\exists!}$; la negación de $\exists^\circ$, esto es, $\neg\exists^\circ$, se nota a veces $\nexists^\circ$ o por $\overline{\exists^\circ}$.

§ 4.1.4 Satisfactibilidad y validez

Definición 4.18.— De forma análoga a la lógica de juntores, decimos que una fórmula de la lógica de primer orden es *satisfactible* —o, sinónimamente, *posible*— precisamente si es verdadera en alguna de sus interpretaciones.

Definición 4.19.— Decimos que una fórmula de la lógica de primer orden es *válida* —también decimos que es una *verdad lógica*—, precisamente si es verdadera en todas sus posibles interpretaciones.

Ejemplo 192

Determinemos si son satisfactibles o válidas las fórmulas:

0. $\exists x \forall y Pxy \to \forall y \exists x Pxy$;
1. $\forall y \exists x Pxy \to \exists x \forall y Pxy$.

Resolución.—

[5] Si utilizamos $\exists$, necesitamos incorporar la igualdad; en realidad, este cuantor pertenece a la lógica de primer orden con identidad (*cfr. infra* ejemplo 5.6.0 [pág. 423 de esta edición]); $\exists! x(Px \wedge Qx)$ es una abreviatura de $\exists x(Px \wedge Qx \wedge \forall y(Px \wedge Qy \to y = x))$.

[6] $\exists^\circ x(Px \wedge Qx)$ es una abreviatura de $\exists x(Px \wedge Qx) \wedge \exists x(Px \wedge \neg Qx)$.

0. La fórmula $\exists x \forall y Pxy \rightarrow \forall y \exists x Pxy$ es válida debido a que no existe ninguna interpretación en la que sea falsa;[7]

1. la fórmula $\forall y \exists x Pxy \rightarrow \exists x \forall y Pxy$ —la conversa de la anterior— es satisfactible pero no es válida, ya que, por ejemplo, es falsa en la interpretación con universo el de los números naturales mayores que uno y $Pxy \leftrightharpoons x$ divide a y. ■

Teorema 4.0 (Validez y dominio de interpretación)

0. Una fórmula es válida en un dominio de interpretación no vacío precisamente si su negación no es posible en ese dominio.
1. Una fórmula es válida precisamente si su negación no es posible.
2. Si una fórmula es posible en un dominio no vacío, entonces es posible en cualquier universo no vacío de igual o mayor cardinal.
3. Si una fórmula es válida en un dominio no vacío, entonces es válida en cualquier universo no vacío de igual o menor cardinal.

Definición 4.20.— Decimos que Φ es un *conjunto finitamente satisfactible de fórmulas* precisamente si todos los subconjuntos finitos de fórmulas de Φ son satisfactibles.

Teorema 4.1 (Teorema de compacidad)
Un conjunto de fórmulas es satisfactible si, y sólo si, es finitamente satisfactible.

§ 4.1.5 Implicación, contradicción y contingencia lógicas

Los conceptos y resultados estudiados en § 1.10 (pág. 145 de esta edición) y en § 1.12 (pág. 156 de esta edición) son válidos para la lógica de cuantores.

Ejemplo 193

Dos cuestiones:

0. ¿es $\forall y \exists x Pxy$ consecuencia lógica de $\exists x \forall y Pxy$?;
1. ¿es $\exists x \forall y Pxy$ consecuencia lógica de $\forall y \exists x Pxy$?

Resolución.— Por lo estudiado en el ejemplo 192 (pág. 377 de esta edición), se sigue que:

0. $\exists x \forall y Pxy \vDash \forall y \exists x Pxy$;

1. $\forall y \exists x Pxy \nvDash \exists x \forall y Pxy$. ■

[7] Más preciso hubiese sido haber dicho que no existe ninguna interpretación con universo no vacío en la que sea falsa.

§ 4.1.6 Equivalencia lógica

Los conceptos y resultados estudiados en § 1.13 (pág. 156 de esta edición), son válidos para la lógica de cuantores.

Ejemplo 194

¿Es posible reescribir la fórmula $\forall x\,(\exists y\,(Pxy \wedge Qxy) \rightarrow Rx)$ —B en el ejemplo 182 (pág. 369 de esta edición)—como $\forall z\,(\exists w\,(Pzw \wedge Qzw) \rightarrow Rz)$?

Resolución.— Sí, puesto que es posible reescribirla renombrando una variable de sujeto, bien $\forall z\,(\exists y\,(Pzy \wedge Qzy) \rightarrow Rz)$, bien $\forall x\,(\exists w\,(Pxw \wedge Qxw) \rightarrow Rx)$, pero también renombrando ambas, $\forall z\,(\exists w\,(Pzw \wedge Qzw) \rightarrow Rz)$; todas ellas son fórmulas equivalentes, pues dada una interpretación el valor de verdad de la fórmula original y las reescritas es el mismo; esto sucede porque todas las variables están en el alcance de algún cuantor. ■

Ejemplo 195

Formulemos en lógica de primer orden las transformaciones de los juicios del ejemplo 40 (pág. 25 de esta edición).

Resolución.—

- Transformación en su contradictorio (negación del universal) (*prae contradic*); por ejemplo AO: de «toda verdad es para ser dicha» (A) obtenemos «no toda verdad es para ser dicha» que es equivalente a «alguna verdad no es para ser dicha» (O), es decir,

$$\forall xPx \dashrightarrow \neg\forall xPx \equiv \exists x\neg Px.$$

- Transformación en su contrario (negación de lo afirmado) (*post contra*); por ejemplo AE: de «toda verdad es para ser dicha» (A) obtenemos «toda verdad no es para ser dicha» que es equivalente a «ninguna verdad es para ser dicha» (E), es decir,

$$\forall xPx \dashrightarrow \forall x\neg Px \equiv \neg\exists xPx.$$

- Transformación en su subalternante (negación simultánea del existencial y de lo afirmado) (*prae-post-que subalter*); por ejemplo IA: de «alguna verdad es para ser dicha» obtenemos «no hay verdad que no sea para ser dicha» que es equivalente a «toda verdad es para ser dicha», es decir,

$$\exists xPx \dashrightarrow \neg\exists x\neg Px \equiv \forall xPx.$$ ■

Por otro lado, en el mismo ejemplo nos preguntábamos si era posible en el caso de la subcontrariedad, igual, con la negación; esto, formulado en el lenguaje de primer orden, es

$$\exists x Px \dashrightarrow \text{¿?} \equiv \exists x \neg Px.$$

De hecho, los cuantores universal y existencial se relacionan así[8]:

$$\begin{aligned} \text{Definición del generalizador (DG):} &\quad \forall x Px \;=\!\mid\models\; \neg\exists x \neg Px; \\ \text{Negación del generalizador (NG):} &\quad \neg\forall x Px \;=\!\mid\models\; \exists x \neg Px; \\ \text{Definición del particularizador (DP):} &\quad \exists x Px \;=\!\mid\models\; \neg\forall x \neg Px; \\ \text{Negación del particularizador (NP):} &\quad \neg\exists x Px \;=\!\mid\models\; \forall x \neg Px. \end{aligned}$$

De este modo, es suficiente un cuantor y el juntor $\neg$ para definir el otro, lo cual nos llevará a definir el concepto de base de cuantores[9].

Ejemplo 196

Formulemos en lógica de primer orden la equivalencia de los juicios 'toda verdad es para ser dicha' y 'no hay ninguna verdad que no sea para ser dicha' vista en el ejemplo 36 (pág. 22 de esta edición).

Resolución.— Su formulación como proposiciones en lógica de primer orden es $\forall x Px$ y $\neg\exists x \neg Px$, respectivamente. Ambas proposiciones son equivalentes. ■

Observación 4.1.6.— Desde la semántica —teoría de modelos—, sería posible estudiar en este momento muchas más equivalencias lógicas, así como sus correspondientes fórmulas válidas, pero quizás sea mejor dejar para más adelante su presentación y hacerla desde la sintaxis —teoría de la demostración—, como reglas deductivas dobles, cosa que hacemos en el capítulo 5 (pág. 398 de esta edición).

§ 4.1.7 Base de cuantores

Por lo comentado en el epígrafe precedente y de manera similar a como en lógica de juntores hablamos de base de juntores y en la lógica de circuitos combinacionales de base de compuertas lógicas, hablaremos en la LPO de base de cuantores.

Definición 4.21.— Decimos que un conjunto de cuantores es una *base de cuantores* (bac) (o, sinónimamente, *conjunto adecuado de cuantores/cuantificadores* [caf], *conjunto completamente expresivo de cuan-*

[8] *Cfr. infra* teorema 5.0 (pág. 411 de esta edición), para las abreviaturas DG, NG, DP y NP.
[9] *Vid. infra* § 4.1.7 (pág. 380 de esta edición).

tores/cuantificadores, *conjunto completo de cuantores/cuantificadores* o *conjunto funcionalmente completo de cuantores/cuantificadores*) precisamente si todos los cuantores pueden expresarse en función de tal conjunto.

Son tres las bases de cuantores: una diádica, $\{\exists, \forall\}$, y dos monádicas, $\{\exists\}$ y $\{\forall\}$.

Observación 4.1.7.— En la definición de fórmula[10] de la lógica de primer orden pudiésemos sustituir el conjunto C por cualquier base de cuantores.

§ 4.1.8 Tablas semánticas

Habíamos visto en lógica de juntores que el método de tablas semánticas es en realidad un algoritmo que nos permite decidir la validez de una fórmula o de un argumento. Lo seguirá siendo en el caso de la lógica de primer orden monádica, pero no, al menos no directa ni inmediatamente, en el de la poliádica.

La imposibilidad de mecanizar la lógica, consecuencia del teorema de Church, subyace en la discusión sobre la automatización del método de tablas semánticas en la lógica de cuantores de primer orden, considerada en su totalidad —monádica y poliádica—, ya que las tablas podrían extenderse indefinidamente, precisamente para aquellas fórmulas de la lógica de primer orden poliádica que no son decidibles.

Veamos el método. De manera similar a como hicimos en la lógica de juntores, lo presentamos con *reglas semánticas* y *patrones de extensión*, existiendo una correspondencia biyectiva entre dichas reglas y patrones, hecho que reflejamos al hablar finalmente de reglas de extensión, en este caso, además de las reglas -α y -β, dos nuevas, la regla-γ (para la generalización) y la regla-δ (para la particularización)[11], además de una modificación de esta última, la regla-δ', que nos permitirá encontrar modelos en el caso de árboles que se extiendan infinitamente[12].

Reglas semánticas

Recordemos que en la presentación como reglas semánticas utilizamos:

- el signo $\diagup\diagdown$ para indicar que se bifurca la inferencia en dos expresiones alternativas, de los cuales, al menos una, ha de ser verdadera;
- el signo | para indicar que la inferencia se compone de dos expresiones, ambas verdaderas.

Como en L_0 —*vid. supra* § 3.3.0 (pág. 275 de esta edición)—, en L_1 también agrupamos las reglas semánticas en reglas semánticas de verdad y reglas semánticas de falsedad. Tanto para unas como

[10] *Cfr. supra* definición 4.2 (pág. 366 de esta edición).
[11] *Cfr. infra* § 366 (pág. 384 de esta edición).
[12] *Cfr. infra* § 366 (pág. 389 de esta edición).

para otras, añadimos dos reglas nuevas a las ya estudiadas a la lógica de juntores, a saber, las correspondientes a la generalización y a la particularización. De este modo, para la lógica de primer orden, tenemos las siguientes seis reglas de verdad y siete reglas de falsedad.

Reglas semánticas de verdad en L₁

Verdad de la disyunción (VD):

$$\frac{\phi \lor \psi}{\phi \quad \big| \quad \psi}$$

(se ramifica en ϕ y ψ)

Verdad de la conjunción (VC):

$$\frac{\phi \land \psi}{\begin{array}{c}\phi \\ | \\ \psi\end{array}}$$

Verdad de la implicación (VI) —Principio de FILÓN—:

$$\frac{\phi \to \psi}{\neg\phi \quad \big| \quad \psi}$$

(se ramifica en $\neg\phi$ y ψ)

Verdad de la equivalencia (VE):

$$\frac{\phi \leftrightarrow \psi}{(\phi \land \psi) \quad \big| \quad (\neg\phi \land \neg\psi)}$$

(se ramifica en $(\phi \land \psi)$ y $(\neg\phi \land \neg\psi)$)

Verdad de la generalización (VG):

$$\frac{\forall x \phi x}{\phi t}$$

(t es un término anterior o un parámetro cualquiera —si no existe tal término—)

Verdad de la particularización (VP) —Regla de instanciación existencial (RIE)—:

$$\frac{\exists x \phi x}{\phi a}$$

(a es un parámetro nuevo)

Reglas semánticas de falsedad en L₁

Falsedad de la negación (FN) —Doble negación (DN)—:

$$\frac{\neg\neg\phi}{\phi}$$

Falsedad de la disyunción (FD) —Ley de DE MORGAN DM_0—:

$$\frac{\neg(\phi \lor \psi)}{\begin{array}{c}\neg\phi \\ | \\ \neg\psi\end{array}}$$

Falsedad de la conjunción (FC)
—Ley de De Morgan DM_1—:

$$\frac{\neg(\phi \wedge \psi)}{\neg\phi \qquad \neg\psi}$$

Falsedad de la implicación (FI)
—Principio de Crisipo—:

$$\frac{\neg(\phi \rightarrow \psi)}{\begin{array}{c}\phi \\ | \\ \neg\psi\end{array}}$$

Falsedad de la equivalencia (FE):

$$\frac{\neg(\phi \leftrightarrow \psi)}{(\phi \wedge \neg\psi) \qquad (\neg\phi \wedge \psi)}$$

Falsedad de la generalización (FG):

$$\frac{\neg\forall x \phi x}{\neg\phi a}$$ (a es un parámetro nuevo)

Falsedad de la particularización (FP):

$$\frac{\neg\exists x \phi x}{\neg\phi t}$$ (t es un término anterior o un parámetro cualquiera —si no existe tal término—)

Patrones de extensión

Dadas la base de juntores $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ y la base de cuantores $\{\exists, \forall\}$, son los siguientes.

Patrones de extensión de tipo α en L_1 (los mismos que en L_0)

Para las fórmulas-α, aquéllas en las que el signo principal es $\wedge$.

	α	α_0	α_1
Falsedad de la negación (FN):	$\neg\neg\phi$	ϕ	ϕ
Verdad de la conjunción (VC):	$\phi \wedge \psi$	ϕ	ψ
Falsedad de la disyunción (FD):	$\neg(\phi \vee \psi)$	$\neg\phi$	$\neg\psi$
Falsedad de la implicación (FI):	$\neg(\phi \rightarrow \psi)$	ϕ	$\neg\psi$

Patrones de extensión de tipo β en L_1 (los mismos que en L_0)

Para las fórmulas-β, aquéllas en las que el signo principal es $\vee$.

	β	β_0	β_1
Falsedad de la conjunción (FC):	$\neg(\phi \wedge \psi)$	$\neg\phi$	$\neg\psi$
Verdad de la disyunción (VD):	$\phi \vee \psi$	ϕ	ψ
Verdad de la implicación (VI):	$\phi \rightarrow \psi$	$\neg\phi$	ψ
Verdad de la equivalencia (VE):	$\phi \leftrightarrow \psi$	$\phi \wedge \psi$	$\neg\phi \wedge \neg\psi$
Falsedad de la equivalencia (FE):	$\neg(\phi \leftrightarrow \psi)$	$\phi \wedge \neg\psi$	$\neg\phi \wedge \psi$

Patrones de extensión de tipo γ en L_1

Para las fórmulas-γ, aquéllas en las que el signo principal es $\forall$.

	γx	γt
Verdad de la generalización (VG):	$\forall x \phi x$	ϕt
Falsedad de la particularización (FP):	$\neg\exists x \phi x$	$\neg\phi t$

Patrones de extensión de tipo δ en L_1

Para las fórmulas-δ, aquéllas en las que el signo principal es $\exists$.

	δx	δt
Verdad de la particularización (VP):	$\exists x \phi x$	ϕa
Falsedad de la generalización (FG):	$\neg\forall x \phi x$	$\neg\phi a$

Como intuimos y apreciamos, hay una correspondencia biyectiva entre las reglas semánticas y los patrones de extensión.

Reglas de extensión

Para reflejar, en cierta forma, la equivalencia entre reglas semánticas y patrones de extensión, hablamos de *reglas de extensión*.

Definición 4.22.— Como sabemos, las reglas juntoriales de extensión α y β permiten extender un árbol, introduciendo subfórmulas de las fórmulas que etiquetan nodos de dicho árbol.

Regla-α: Si la fórmula-α tiene la estructura $\alpha_0 \wedge \alpha_1$, extendemos ρ con dos nuevos nodos consecutivos α_0 y α_1 (si $\alpha_0 = \alpha_1$, sólo añadimos un nodo).

Regla-β: Si la fórmula-β tiene la estructura $\beta_0 \vee \beta_1$, extendemos ρ con dos nuevos nodos, uno izquierdo y otro derecho, β_0 y β_1, esto es, obtenemos dos subramas (si $\beta_0 = \beta_1$, sólo añadimos un nodo).

En LPO se añaden dos nuevas, las reglas cuantoriales de extensión γ y δ.

Regla-γ: Si la fórmula-γ tiene la estructura $\forall x\phi x$, extendemos ρ con un nuevo nodo ϕt (instancia con el término t de la matriz cuantorial de $\forall x\phi x$), y si la fórmula-γ tiene la estructura $\neg\exists x\phi x$, extendemos ρ con un nuevo nodo $\neg\phi t$ (instancia con el término t de la matriz cuantorial de $\neg\exists x\phi x$), siendo, en ambos casos, t, un término que aparece en la rama (o un parámetro cualquiera, caso de no existir tal término).

Regla-δ: Si la fórmula-δ tiene la estructura $\exists x\phi x$, extendemos ρ con un nuevo nodo ϕa (instancia con el parámetro a de la matriz cuantorial de $\exists x\phi x$), y si la fórmula-δ tiene la estructura $\neg\forall x\phi x$, extendemos ρ con un nuevo nodo $\neg\phi a$ (instancia con el parámetro a de la matriz cuantorial de $\neg\forall x\phi x$), siendo, en ambos casos, a, un parámetro que no aparece antes en la rama.

La *guía para la aplicación de las reglas de extensión α, β, γ y δ* se resume en las instrucciones:

0.ª, la regla-α sólo se aplica una vez a cada nodo que contenga una fórmula-α, tras lo que se anota, este nodo origen con el signo $\surd_n$, siendo n el identificador del nodo creado, y el nodo creado se anota con este identificador y con la abreviatura de la regla aplicada junto al identificador del nodo origen;

1.ª, la regla-β sólo se aplica una vez a cada nodo que contenga una fórmula-β, tras lo que se anotan, este nodo origen con el signo $\surd_{m,n}$, siendo m y n los identificadores de los nodos creados, y los nodos creados se anotan con estos identificadores y con la abreviatura de la regla aplicada junto al identificador del nodo origen;

2.ª, la regla-δ sólo se aplica una vez a cada nodo que contenga una fórmula-δ, tras lo que se anota, este nodo origen con el signo $\surd_{\langle n,a_k\rangle}$, siendo n el identificador del nodo creado y a_k el parámetro usado, y el nodo creado se anota con este identificador n y con la abreviatura de la regla aplicada junto al identificador del nodo origen;

3.ª, si la fórmula-γ de donde proviene una fórmula en la que figura un parámetro no está anotada con éste, ha de aplicarse la regla-γ a dicha fórmula-γ (ya que ésta se satisface para aquél); esto hace que la regla-γ pudiese aplicarse indefinidamente —tantas veces como parámetros tenga el lenguaje formal (LPO tiene un número numerable de parámetros que llamamos a_0, a_1, a_2, ...)—; tras cada aplicación de la regla-γ a un nodo, se anota este nodo origen con el signo $\surd_{\langle n,t\rangle}$, siendo n el identificador del nodo creado y t el término usado, y el nodo creado se anota con este identificador n y con la abreviatura de la regla aplicada junto al identificador del nodo origen;

4.ª, la regla-α tiene prioridad sobre la regla-β;

5.ª, las reglas juntoriales (α y β) tienen prioridad sobre las reglas cuantoriales (γ y δ);

6.ª, la regla-δ tiene prioridad sobre la regla-γ, y

7.ª, una vez demostrada la insatisfactibilidad de una rama, se etiqueta con el signo $\times$ y no se extiende más.

Teorema 4.2

En la lógica de primer orden, TA/S es un sistema consistente (toda fórmula demostrable mediante TA/S es una fórmula válida) y completo (toda fórmula válida es demostrable mediante TA/S).

Muestra de ejemplos

El siguiente ejemplo muestra la acción de TA/S sobre una fórmula válida en la LPO monádica.

Ejemplo 197

Ha sido establecido que a quien lo haga se le premia. Resulta que lo ha hecho una persona. Entonces, ha de premiarse a una persona, ¿verdad?

[Cubit 44].

Resolución.—

Formalización de $\mathcal{A}$ en lógica de de primer orden.

- *Variables proposicionales*:

  Siendo el universo de discurso el conjunto de todas las personas, consideremos los siguientes predicados:

  $Px \leftrightharpoons$ x lo hace;

  $Qx \leftrightharpoons$ se premia a x.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\forall x(Px \to Qx), \exists xPx\}$ y la conclusión ψ, a saber, $\exists xQx$.

  La fórmula correspondiente a en lógica de primer orden es $\forall x(Px \to Qx) \land \exists xPx \to \exists xQx$.

  Construcción anotada del árbol semántico.

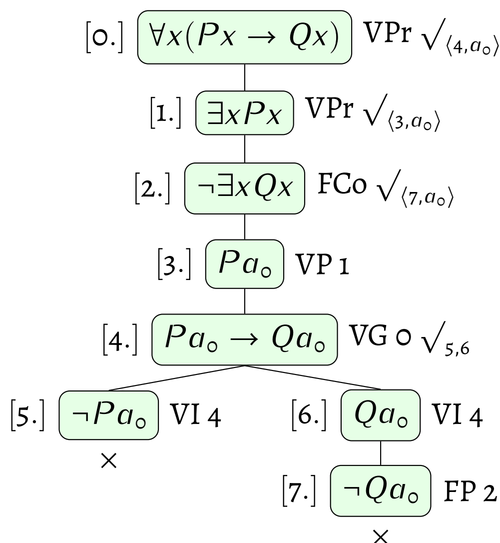
La construcción del árbol comienza escribiendo las premisas en los nodos 0 y 1 y la negación de la conclusión en el nodo 2 y anotando dichos nodos con VPr (Verdad de la premisa) los dos primeros y FCo (Falsedad de la conclusión) el último. Éstas son las tres únicas asunciones. Ninguna de ellas lleva aún marca de su utilización en la generación de fórmulas siguientes ni de uso de términos o parámetros en éstas.

Como las de 0 y 2 son fórmulas-γ y la de 1 es una fórmula-δ, comenzamos por esta última, aplicándole la regla-δ Verdad de la particularización (VP), teniendo en cuenta que como no aparece ningún parámetro en las fórmulas precedentes en la rama, sustituimos x por el primero de los parámetros, a_0, por lo que escribimos la fórmula en el nodo 3 como una instancia con dicho parámetro de la matriz cuantorial de la fórmula de 1, anotando en este momento el nodo 3 con la información de la procedencia de su fórmula, VP 1, y anotando el nodo 1 con la marca de utilización en 3 y el uso del parámetro a_0, que abreviamos por $\surd_{\langle 3, a_0 \rangle}$.

Al no quedar ninguna fórmula-δ, seguimos por la fórmula de 0, a la que aplicamos la regla-γ Verdad de la generalización (VG), y teniendo en cuenta que el término a_0 ya ha aparecido, sustituimos x por a_0, por lo que escribimos la fórmula en el nodo 4 como una instancia con dicho parámetro de la matriz cuantorial de la fórmula de 0, anotando ahora el nodo 4 con la información de la procedencia de su fórmula, VG 0, y anotando el nodo 0 con la marca de utilización en 4 y el uso del parámetro a_0, que abreviamos por $\surd_{\langle 4, a_0 \rangle}$.

Aplicamos la regla-β Verdad de la implicación (VI) a la fórmula de 4, obteniendo dos subramas con sendos literales, escribiendo uno en el nodo 5 y otro en el nodo 6, anotando ambos con la información de la procedencia de sendos literales, VI 4, y anotando el nodo 4 con la marca de utilización en 5 y 6, $\surd_{5,6}$. Resulta, en cualquier caso, que el literal de 5 ($\neg Pa_0$) es complementario del literal de 3 (Pa_0), por lo que la rama 0 — 5 es insatisfactible.

La única fórmula que queda es la del nodo 2, a la que aplicamos la regla-γ Falsedad de la particularización (FP) y como el término a_0 ya ha aparecido, sustituimos x por a_0, por lo que escribimos la fórmula en el nodo 7 como una instancia con dicho parámetro de la matriz cuantorial de la fórmula de 2, anotando ahora el nodo 7 con la información de la procedencia de su fórmula, FP 2, y anotando el nodo 2 con la marca de utilización en 7 y el uso del parámetro a_0, abreviadamente $\surd_{\langle 7, a_0 \rangle}$. Como el literal del nodo 7 ($\neg Qa_0$) y el literal del nodo 6 (Qa_0) son complementarios, la rama 0 — 7 es insatisfactible.



Observación.— VPr $\leftrightharpoons$ Verdad de la premisa; FCo $\leftrightharpoons$ Falsedad de la conclusión; VP $\leftrightharpoons$ Verdad de la particularización (regla-δ); VG $\leftrightharpoons$ Verdad de la generalización (regla-γ); VI $\leftrightharpoons$ Verdad de la implicación (regla-β); FP $\leftrightharpoons$ Falsedad de la particularización (regla-γ).

Decisión sobre la validez de la fórmula.

Este árbol tiene sólo dos ramas, ambas insatisfactibles, por lo que es un árbol terminado. Observemos que esto es consistente con el hecho de que ambas fórmulas-γ están anotadas con el único parámetro presente en el árbol, a_0, por lo que no hay necesidad de aplicar de nuevo ninguna regla-γ.

Por lo tanto, $\forall x(Px \to Qx) \wedge \exists x Px \to \exists x Qx$ es una fórmula válida y como la lógica de primer orden es completa[13], $\forall x(Px \to Qx) \wedge \exists x Px \to \exists x Qx$ es un teorema lógico, en otras palabras[14], $\forall x(Px \to Qx) \wedge \exists x Px \vdash \exists x Qx$. ■

El siguiente ejemplo muestra la acción de TA/S sobre una fórmula en la LPO diádica, surgiendo un problema, el árbol es infinito.

Ejemplo 198

Acordamos formalizar «No importa qué dato se ingrese en el programa, siempre habrá al menos un resultado posible. Perdón, quisimos decir justamente lo contrario.» por $\neg\forall x \exists y Pxy$; intentemos deducir por TA/S si se trata de una fórmula válida.

[Cubit 45].

Resolución.—

Construcción anotada del árbol semántico.

La construcción del árbol comienza escribiendo la negación de la fórmula en el nodo 0, anotando dicho nodo con FF (Falsedad de la fórmula). Ésta es la única asunción. No lleva aún marca de su utilización en la generación de fórmulas siguientes ni de uso de términos o parámetros en éstas. Le aplicamos la regla α Falsedad de la negación (FN), por lo que escribimos la fórmula en 1, anotando en este momento el nodo 1 con la información la procedencia de su fórmula, FN 0, y anotando el nodo 0 con la marca de utilización de su fórmula en 1.

Resulta una fórmula-γ en 1, a la que aplicamos la regla-γ Verdad de la generalización (VG) y teniendo en cuenta que como no aparece ningún término en las fórmulas precedentes en la rama, sustituimos x por el primero de los parámetros, a_0, por lo que escribimos la fórmula en el nodo 2 como una instancia con dicho parámetro de la matriz cuantorial de la fórmula de 1, anotando en este momento el nodo 2 con la información de la procedencia de su fórmula, VG 1, y anotando el nodo 1 con la marca de utilización en 2 y el uso del parámetro a_0, que abreviamos por $\surd_{\langle 2, a_0 \rangle}$.

---

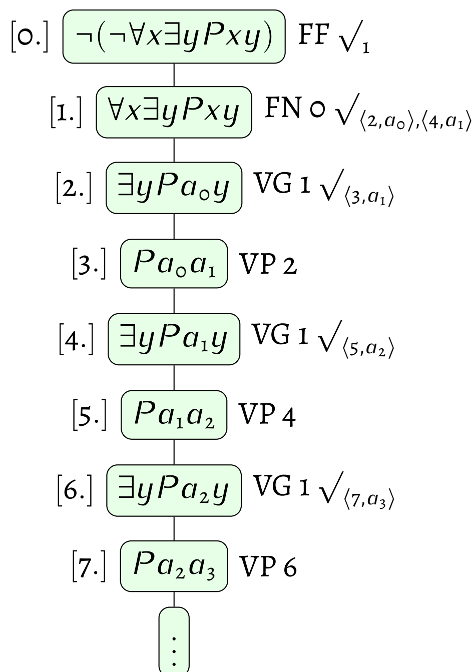
[13] *Vid. infra* teorema 6.11 (pág. 452 de esta edición).
[14] *Vid. infra* observación 2.1.3 (pág. 189 de esta edición).

Resulta una fórmula-δ en 2, a la que aplicamos la regla-δ Verdad de la particularización (VP), sustituyendo x por un parámetro que no haya aparecido en la rama, digamos a_1, por lo que escribimos la fórmula en el nodo 3 como una instancia con dicho parámetro de la matriz cuantorial de la fórmula de 2, anotando en este momento el nodo 3 con la información de la procedencia de su fórmula, VP 2, y anotando el nodo 2 con la marca de utilización en 3 y el uso del parámetro a_1, que abreviamos por $\surd_{\langle 3,a_1\rangle}$.

Como la fórmula-γ de donde en origen proviene la fórmula en 3, a saber, la fórmula en 1, no está anotada con a_1, debemos aplicar otra vez la regla-γ Verdad de la generalización (VG) a dicha fórmula en 1, eligiendo como parámetro precisamente a_1 para poder anotarla con él, por lo que escribimos la fórmula en el nodo 4 como una instancia con dicho parámetro de la matriz cuantorial de la fórmula de 1, anotando en este momento el nodo 4 con la información de la procedencia de su fórmula, VG 1, y anotando el nodo 1 con la marca de utilización en 4 y el uso del parámetro a_1, que abreviamos por $\surd_{\langle 4,a_1\rangle}$.

Y así sucesivamente.

La infinitud del árbol se debe a la ausencia en la fórmula del nodo 1 de marca de utilización de cada nuevo parámetro.



Observación.— FF $\leftrightharpoons$ Falsedad de la fórmula; FN $\leftrightharpoons$ Falsedad de la negación (regla-α); VG $\leftrightharpoons$ Verdad de la generalización (regla-γ); VP $\leftrightharpoons$ Verdad de la particularización (regla-δ). ■

Modificación de la Regla delta

Esta modificación nos permitirá encontrar modelos en el caso de árboles que se extiendan infinitamente.

Regla-δ': Si la fórmula-δ tiene la estructura $\exists x\phi x$, extendemos ρ con nuevos nodos $\phi a_0, \ldots, \phi a_n$, ϕa_{n+1} (instancias con tales parámetros de la matriz cuantorial de $\exists x\phi x$), y si la fórmula-δ tiene la estructura $\neg\forall x\phi x$, extendemos ρ con nuevos nodos $\neg\phi a_0, \ldots, \neg\phi a_n, \neg\phi a_{n+1}$ (instancias con tales parámetros de la matriz cuantorial de $\neg\forall x\phi x$), siendo, en ambos casos, $a_0, \ldots, a_n$ los parámetros que han aparecido antes en la rama y a_{n+1} un parámetro que no ha aparecido antes en la rama.

Veamos un ejemplo.

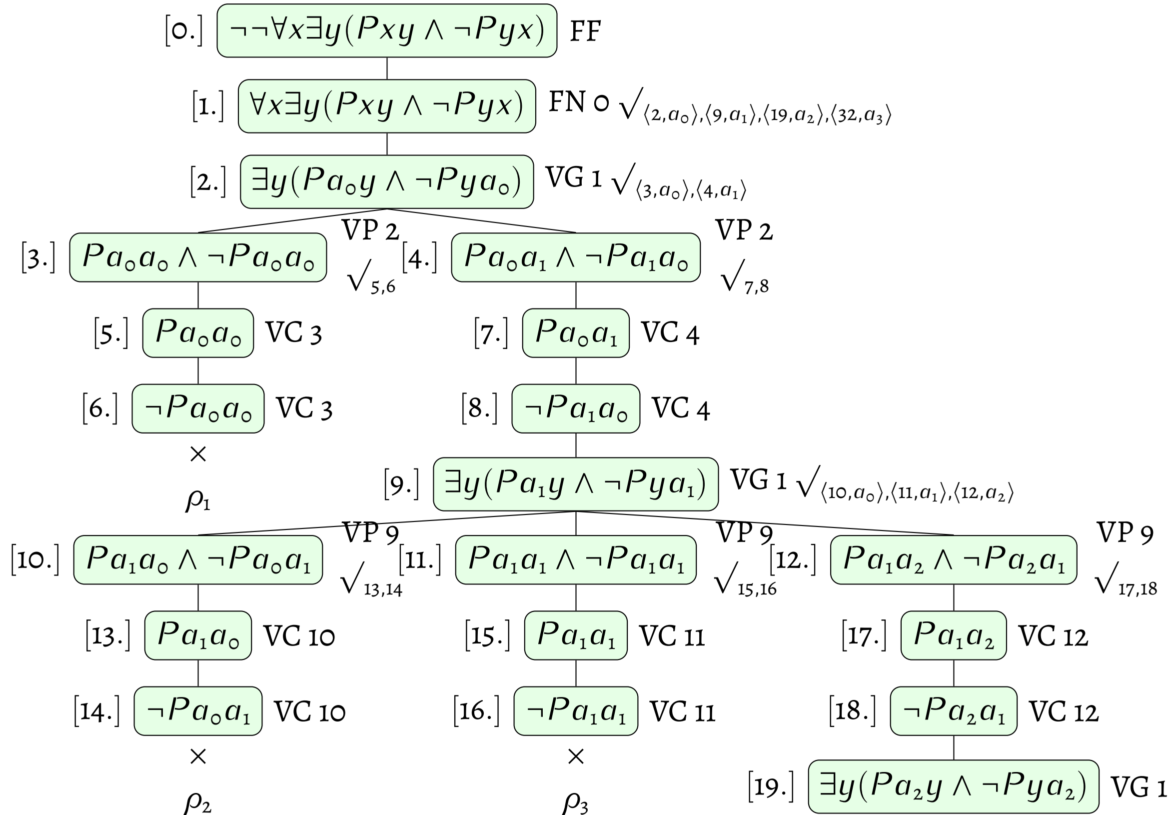
Ejemplo 199

Intentemos deducir por TA/S si es válida la fórmula $\neg\forall x\exists y(Pxy \wedge \neg Pyx)$.

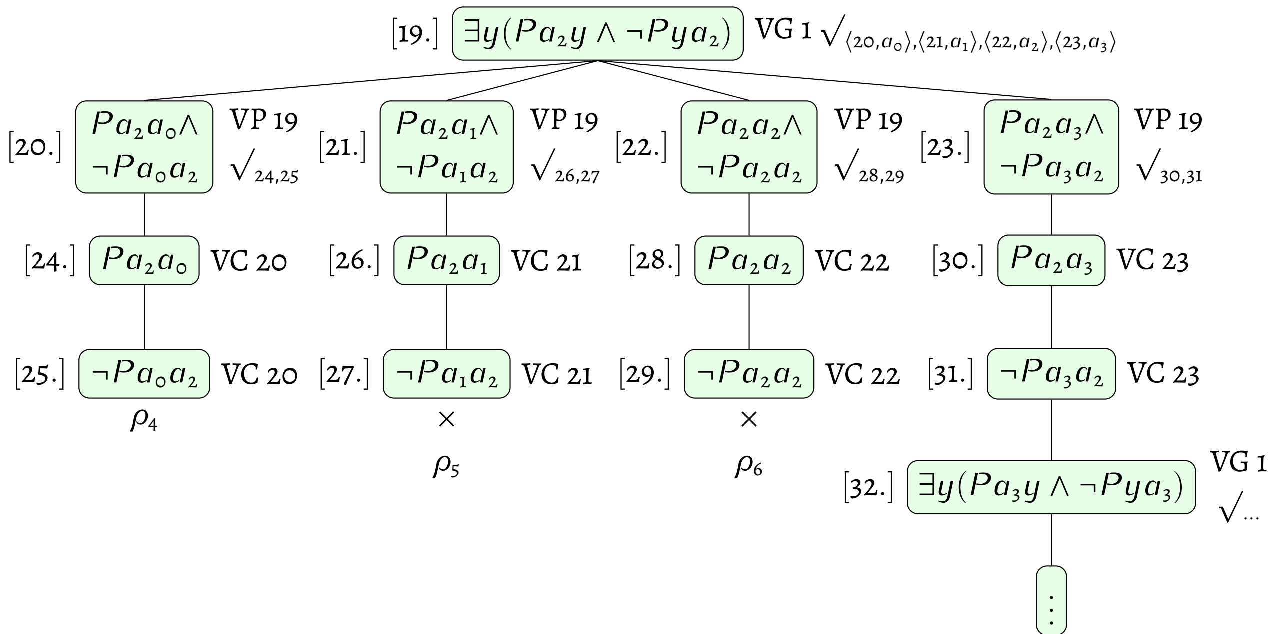
[Cubit 48].

Resolución.—

Construcción anotada del árbol semántico aplicando las reglas -α, -β, -γ y -δ'.



Justo en el siguiente nivel, de [19.] parten cuatro subramas, con nodos cabecera, $Pa_2a_x \wedge \neg Pa_xa_2$, con $x \in \{0, 1, 2, 3\}$, siendo la correspondiente a a_0 una rama satisfactible, las correspondientes a a_1 y a_2 insatisfactibles, continuando el árbol por la correspondiente a a_3 (el nuevo parámetro).



La rama satisfactible, ρ_4, es el conjunto de fórmulas de los nodos 0, 1, 2, 4, 7, 8, 9, 12, 17, 18, 19, 20, 24 y 25.

Esta rama proporciona un modelo para el conjunto decisor $\Gamma = \{\neg\neg\forall x \exists y(Pxy \wedge \neg Pyx)\}$, a saber, el universo de discurso

$$U = \{0, 1, 2\}$$

(los subíndices de los parámetros que aparecen en la rama) y la función de interpretación (que asocia a cada parámetro una entidad de U y a cada signo de predicado una relación de la misma aridad —en este caso, diádica— sobre U—*cfr. supra* definición 4.16 (pág. 373 de esta edición)—)

$$\begin{aligned} I(a_0) &= 0, \\ I(a_1) &= 1, \\ I(a_2) &= 2, \\ I(P) &= \{\langle 0,1\rangle, \langle 1,2\rangle, \langle 2,0\rangle\} \end{aligned}$$

—precisamente éstos porque Pa_0a_1, Pa_1a_2 y Pa_2a_0 están en ρ_4 (nodos 7, 17 y 24, respectivamente; también están en ρ_4, $\neg Pa_1a_0$, $\neg Pa_2a_1$ y $\neg Pa_0a_2$ (nodos 8, 18 y 25, respectivamente) por lo que $\langle 1,0\rangle \notin I(P)$, $\langle 2,1\rangle \notin I(P)$ y $\langle 0,2\rangle \notin I(P)$; como Pa_0a_0, Pa_1a_1 y Pa_2a_2 no están en ningún nodo de ρ_4, $\langle 0,0\rangle$, $\langle 1,1\rangle$ y $\langle 2,2\rangle$ no pertenecen a $I(P)$—.

En definitiva, la fórmula $\neg\forall x \exists y(Pxy \wedge \neg Pyx)$ no es válida.

Notemos, de paso, que la relación que nos ha proporcionado la función de interpretación es una relación circular[15]. ■

[15] *Vid. infra* definición 11.35 (pág. 623 de esta edición).

Observación 4.1.8.— Pudiésemos comprobar este resultado en el artefacto en línea Tree Proof Generator[16] con la petición $\neg\forall x\exists y(Pxy \land \neg Pyx)$.

Actividad 4.0

¿Se nos ocurre una traducción directa de $\neg\forall x\exists y(Pxy \land \neg Pyx)$ a español? (¿Pudiese ésta venir sugerida por la interpretación encontrada en el ejemplo anterior?).

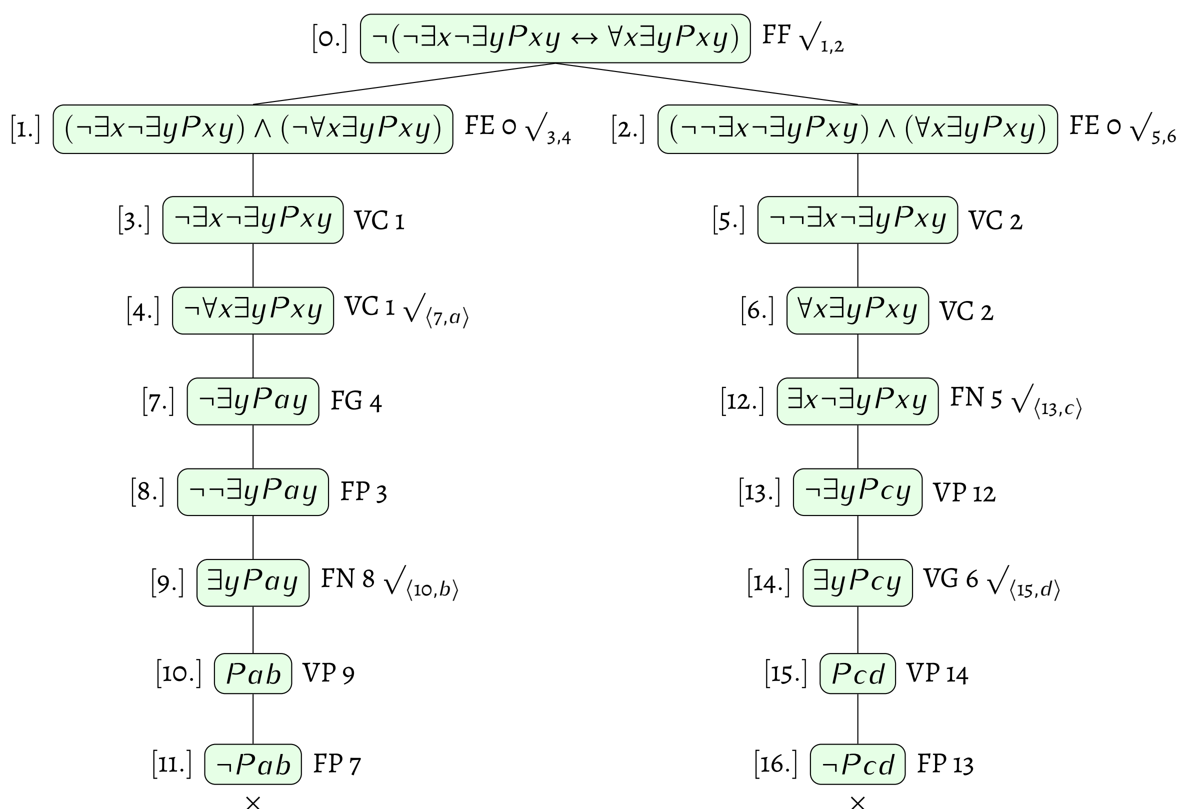
[Cubit 48].

Actividad 4.1

Demostremos por TA/S que $\neg\exists x\neg\exists y Pxy$ equivale a $\forall x\exists y Pxy$.

[Cubit 49].

Con miras a su resolución.— Ésta es la tabla:



Actividad 4.2

Siendo la interpretación $Pxy \leftrightharpoons y$ es el opuesto de x, en el dominio de los números enteros, interpretamos $\neg\exists x\neg\exists y Pxy$ como «no existe ninguna pareja de números enteros en la que uno sea el opuesto del otro» y $\forall x\exists y Pxy$ como «todo número entero tiene un opuesto». Es-

---

[16] *Vid. supra* § 3.3.9 (pág. 319 de esta edición).

tas interpretaciones parecen decir lo contrario y, sin embargo, estas fórmulas son equivalentes —*vid*. la actividad precedente—, ¿cómo es esto posible?

[Cubit 50].

Con miras a su resolución.— Porque la verdadera interpretación de la primera es «no existe ningún entero tal que para él no exista ningún entero que sea su opuesto», en otras palabras, «no existe ningún entero que no tenga opuesto», lo cual, claramente, es lo que afirma la segunda.

Actividad 4.3

Leemos en la especificación de una red que ésta está diseñada de forma que para todo nodo de la misma siempre hay un nodo al que si pudiese enviarle datos —incluso ambos pueden ser el mismo nodo (por ejemplo, vía una dirección de bucle invertido)—, entonces en alguna parte de la red existen al menos dos nodos que tienen un envío de datos bidireccional. Por practicar formalización se nos ha ocurrido expresar esto en LPO: $\forall x \exists y (Pxy \rightarrow \exists z \exists w (Pzw \wedge Pwz))$, donde $Pxy \leftrightharpoons$ el nodo x está conectado al nodo y. Ahora nos preguntamos si ésta es una fórmula válida. Nos proponemos resolverlo utilizando TA/S.

[Cubit 46].

Actividad 4.4

Más adelante en la misma especificación hemos leído algo que hemos formulado en LPO por $\forall x (Qx \rightarrow \exists y Pxy) \rightarrow \forall x (\neg \exists y Pxy \rightarrow \neg Qx)$. De nuevo nos preguntamos si ésta es una fórmula válida, cuestión que nos proponemos resolver utilizando TA/S. Además de esto, ¿se nos ocurre qué pudiésemos haber leído?

[Cubit 47].

Actividad 4.5

La tabla/árbol analítica/semántica (TA/S) de la fórmula $(\forall x (Px \rightarrow Qx) \wedge \forall x (Qx \rightarrow Rx) \wedge \exists x Px) \rightarrow \exists x Rx$, en el que para su construcción hemos hecho uso en todo momento de la guía y heurística para la aplicación de las reglas de extensión, se trata de:

a. un árbol insatisfactible;
b. un árbol satisfactible con sólo una rama satisfactible;
c. un árbol satisfactible con sólo dos ramas satisfactibles;
d. un árbol satisfactible con sólo tres ramas satisfactibles.

[TT].

Actividad 4.6

La tabla/árbol analítica/semántica (TA/S) de la fórmula $(\forall x Px \vee \exists x Qx) \rightarrow \exists x(Px \wedge Qx)$, en el que para su construcción hemos hecho uso en todo momento de la guía y heurística para la aplicación de las reglas de extensión, se trata de:

a. un árbol insatisfactible;
b. un árbol satisfactible con sólo una rama satisfactible;
c. un árbol satisfactible con sólo dos ramas satisfactibles;
d. un árbol satisfactible con sólo tres ramas satisfactibles.

[TT].

Actividad 4.7

La tabla/árbol analítica/semántica (TA/S) de la fórmula $(\forall x \forall y(Pxy \rightarrow Pyx) \wedge \exists x \exists y Lxy) \rightarrow \exists x Lxx$, en el que para su construcción hemos hecho uso en todo momento de la guía y heurística para la aplicación de las reglas de extensión, se trata de:

a. un árbol insatisfactible;
b. un árbol satisfactible con sólo una rama satisfactible;
c. un árbol satisfactible con sólo dos ramas satisfactibles;
d. un árbol con al menos una rama infinita.

[TT].

§ 4.2 Bibliografía

- Para la semántica de la lógica de juntores, en general:
  - Para una primera aproximación:

[62] María Manzano Arjona y Antonia Huertas Sánchez. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

[99] Amador Antón Antón y Pascual Casañ Muñoz. *Lógica matemática. II. Lógica de predicados*. NAU llibres, Valencia, España, 1998.

  - Para estudiar, practicar y conocer más:

[64] Manuel Garrido Giménez. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

[65] Carmen García Trevijano. *El arte de la lógica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1999.

- Para profundizar, acullá:

  [66] Manuel GARRIDO GIMÉNEZ, Luis Manuel VALDÉS VILLANUEVA, Jesús MOSTERÍN DE LAS HERAS, Alfonso GARCÍA SUÁREZ y Carlos-Peregrín FERNÁNDEZ OTERO. *Lógica y lenguaje*. Cuadernos de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1989.

  [67] Raymond Merrill SMULLYAN. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

  [60] Herbert Bruce ENDERTON. *A mathematical introduction to logic*. Harcourt/Academic Press, San Diego, Condado de San Diego, California (US-CA), Estados Unidos de América, 2.ª ed., 2001.

- Para el caso particular de las tablas analíticas/semánticas (TA/S) en la lógica de juntores:

  - Para una primera aproximación:

    [62] María MANZANO ARJONA y Antonia HUERTAS SÁNCHEZ. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

    [99] Amador ANTÓN ANTÓN y Pascual CASAÑ MUÑOZ. *Lógica matemática. II. Lógica de predicados*. NAU llibres, Valencia, España, 1998.

  - Para estudiar, practicar y conocer más:

    [64] Manuel GARRIDO GIMÉNEZ. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

  - Para profundizar, acullá:

    [67] Raymond Merrill SMULLYAN. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

    [90] Evert Willem BETH. *The Foundations of Mathematics. A Study in the Philosophy of Science*. North-Holland, Amsterdam, Países Bajos, 1959.

    [91] Kaarlo Jaakko Juhani HINTIKKA. *The Philosophy of Mathematics*. Oxford, 1969.

    [96] Rafael BENEYTO TORRES. Laberintos analíticos. *Teorema: Revista internacional de filosofía*, 1(4):19–30, 1971.

    [97] Kaarlo Jaakko Juhani HINTIKKA. Form and content in quantification theory. *Acta Philosophica Finnica*, 8:57–55, 1955.

[98] Richard Carl JEFFREY. *Formal Logic: its Scope and Limits*. McGraw-Hill, 1967.

CAPÍTULO 5

Del cálculo de cuantores

Todas las langostas rojas y cocidas están muertas.
Y todas las langostas rojas muertas están cocidas.
Por tanto, todas las langostas muertas cocidas son rojas.

(Lewis CARROLL. *Alicia en el País de las Maravillas*).

La lógica de juntores nos permite representar, analizar y razonar con un reducido número de tipos de declaraciones. En particular no permite representar expresiones como «ninguna entidad», «alguna entidad» o «todas las entidades». Una primera extensión es la lógica de cuantores, que sí nos permite trabajar con ellas. Sin embargo, esta extensión tampoco nos permite representar expresiones como «bastantes entidades» o «muchas entidades».

§ 5.0 Silogística

§ 5.0.0 Silogismo categórico

Si toda persona es un ser con corazón y Cris es una persona, entonces Cris es un ser con corazón.

Hemos hecho una deducción; en efecto, que Cris es un ser con corazón se ha derivado necesariamente del antecedente —una proposición compuesta— de la implicación.

Aristóteles denominó silogismo categórico a esta forma de la derivación.

Definición 5.0.— Un *silogismo categórico* es la expresión verbal del razonamiento deductivo categórico.

En un silogismo categórico existen las *cosas establecidas* —átomos o axiomas, en un antecedente— y la *cosa deducida* —molécula o teorema, en una conclusión—. Las cosas establecidas se denominan *premisa mayor* y *premisa menor* —en el ejemplo, «toda persona es un ser con corazón» y «Cris es una persona», respectivamente—. Estas premisas y la conclusión constituyen la llamada *materia próxima* del silogismo.

Se trata de un *silogismo simple*. También están los polisilogismos, que constan de más de dos premisas, pero su estudio es reducible al de los silogismos simples, pues pueden descomponerse en dos o más de ellos.

Las proposiciones intervinientes, premisas y conclusión, pueden descomponerse en sus términos. Dichas premisas se conectan mediante un término comparador, el llamado *término medio*. En el ejemplo inicial, el término medio es «persona», con el que se comparan «ser con corazón» y «Cris» para concluir que «Cris es un ser con corazón». Se distinguen tres términos en el silogismo categórico: el *término mayor* que forma parte de la premisa mayor y es predicado de la conclusión —en el ejemplo, «ser con corazón»—, el *término medio* que sirve de comparación y el *término menor* que forma parte de la premisa menor y es sujeto de la conclusión. Estos tres términos constituyen la llamada *materia remota* del silogismo.

A los términos menor y mayor se les denomina en su conjunto, *términos extremos*. El término medio es el único que se repite en las premisas y nunca está en la conclusión. En esta última, el término menor desempeña la función de sujeto y el término mayor la de predicado.

Que los silogismos estén bien formados y sean válidos obedece a las reglas del silogismo, las figuras del silogismo y los modos del silogismo.

Las *reglas del silogismo* son ocho, cuatro en cuanto a la materia remota:

0.º, el silogismo consta del término mayor, el medio y el menor (*terminus esto triplex: major mediusque minorque*);

1.º, ni el término mayor ni el menor pueden tener más extensión en la conclusión que en las premisas (*latius hos quam praemissae conclusio non vult*);

2.º, el término medio no forma parte de la conclusión (*nequaquam medium capiat conclusio fas est*);

3.º, el término medio ha de ser universal en al menos una de las premisas (*aut semel aut iterum medius generaliter esto*),

y otras cuatro en cuanto a la materia próxima:

4.º, si las dos premisas son negativas, entonces no existe conclusión (*utraque si praemissa neget, nihil inde sequetur*);

5.º, si las dos premisas son afirmativas, entonces la conclusión no puede ser negativa (*ambae affirmantes nequeunt generare negantem*);

6.º, la conclusión sigue siempre la peor parte (*pejorem sequitur semper conclusio partem*): si una premisa es negativa, entonces la conclusión es negativa; si una premisa es particular, entonces la conclusión es particular;

7.º, si las dos premisas son particulares, entonces no existe conclusión (*nihil sequitur geminis ex particularibus unquam*).

Las *figuras del silogismo* son cuatro (silogística aristotélica[0] —figuras primera, segunda y tercera— y medieval[1] —más la cuarta figura—), dependiendo de la situación del término medio (M) en las premisas (S es el término menor y P el término mayor):

I.ª figura	II.ª figura
M es P	P es M
S es M	S es M
$\therefore$ S es P	$\therefore$ S es P

III.ª figura	IV.ª figura
M es P	P es M
M es S	M es S
$\therefore$ S es P	$\therefore$ S es P

Los *modos del silogismo* son 256. En efecto: tanto las premisas como la conclusión son proposiciones categóricas; recordemos que A, E, I, O denotan las clases de proposiciones categóricas

[0] *Cfr. v. gr.* Smith [100].

[1] Cuarta figura o figura galénica (de Claudio Galeno Nicon de Pérgamo), también conocida como *primera figura indirecta* (al ser admitida por algunos lógicos aristotélicos) —*cfr. v. gr.* Lagerlund [101]—.

—estudiadas en § 0.4.3 (pág. 35 de esta edición)—; para la premisa mayor, la premisa menor y la conclusión, para cada una de ellas existen, por tanto, cuatro posibilidades, por lo que para cada figura existen, por el principio de multiplicación —*vid. infra* § 19.1.1 (pág. 1138 de esta edición)—, $4 \times 4 \times 4 = 64$ posibilidades; como son cuatro las figuras, existe un total de $64 \times 4 = 256$ modos del silogismo.

En ambas silogísticas, aristotélica y medieval, se supone que los términos menor, medio y mayor siempre se refieren a entidades que existen. De aquí que resulten 24 modos válidos, seis para cada una de las cuatro figuras.

El punto de vista mayoritario actual permite que los términos se refieran a entidades existentes o imaginarias. Esto lleva a que ciertos modos de esos 24 sean inválidos. Un ejemplo es *dArAptI*.

Los 19 modos principales de las cuatro figuras son los siguientes:

I.ª figura	Modos principales ($X, Y, Z \in \{ A, E, I, O \}$)		
M es P	Xmp	$Xmp, Ysm \vdash Zsp$	
S es M	Ysm	$Amp, Asm \vdash Asp$	(bArbArA)
$\therefore$ S es P	$\therefore$ Zsp	$Emp, Asm \vdash Esp$	(cElArEnt)
		$Amp, Ism \vdash Isp$	(dArII)
		$Emp, Ism \vdash Osp$	(fErIO)
II.ª figura	**Modos principales ($X, Y, Z \in \{ A, E, I, O \}$)**		
P es M	Xpm	$Xpm, Ysm \vdash Zsp$	
S es M	Ysm	$Epm, Asm \vdash Esp$	(cEsArE)
$\therefore$ S es P	$\therefore$ Zsp	$Apm, Esm \vdash Esp$	(cAmEstrEs)
		$Epm, Ism \vdash Osp$	(fEstInO)
		$Apm, Osm \vdash Osp$	(bArOcO)
III.ª figura	**Modos principales ($X, Y, Z \in \{ A, E, I, O \}$)**		
M es P	Xmp	$Xmp, Yms \vdash Zsp$	
M es S	Yms	$Amp, Ams \vdash Isp$	(dArAptI)
$\therefore$ S es P	$\therefore$ Zsp	$Emp, Ams \vdash Osp$	(fElAptOn)
		$Amp, Ims \vdash Isp$	(dAtIsI)
		$Imp, Ams \vdash Isp$	(dIsAmIs)
		$Omp, Ams \vdash Osp$	(bOcArdO)
		$Emp, Ims \vdash Osp$	(fErIsOn)
IV.ª figura	**Modos principales ($X, Y, Z \in \{ A, E, I, O \}$)**		
P es M	Xpm	$Xpm, Yms \vdash Zsp$	
M es S	Yms	$Apm, Ams \vdash Isp$	(brAmAntIp/bAmAlIp)
$\therefore$ S es P	$\therefore$ Zsp	$Apm, Ems \vdash Esp$	(cAmEnEs/cAlEmEs)
		$Ipm, Ams \vdash Isp$	(dImArIs/dImAtIs)
		$Epm, Ams \vdash Osp$	(fEsApO)
		$Epm, Ims \vdash Osp$	(frEsIsOn)

Actividad 5.0

La expresión de Celarent (Emp, A$sm \vdash$ Esp) en el lenguaje de la lógica de primer orden es

$$\forall x(Mx \to \neg Px) \land \forall x(Sx \to Mx) \to \forall x(Sx \to \neg Px).$$

Formalice los 18 modos principales restantes en el lenguaje de la lógica de primer orden.

A estos 19 modos principales, se les añaden otros cinco llamados *modos subalternos*, que tienen una proposición categórica particular como conclusión:

I.ª figura	Modos subalternos ($X, Y, Z \in \{$ A, E, I, O $\}$)			
		$Xmp, Ysm \vdash Zsp$		
M es P	Xmp	Amp, A$sm \vdash$ Isp	(bArbArI)	
S es M	Ysm	Emp, A$sm \vdash$ Osp	(cElArOnt)	
$\therefore$ S es P	$\therefore$ Zsp			

II.ª figura	Modos subalternos ($X, Y, Z \in \{$ A, E, I, O $\}$)			
		$Xpm, Ysm \vdash Zsp$		
P es M	Xpm	Epm, A$sm \vdash$ Osp	(cEsArO)	
S es M	Ysm	Apm, E$sm \vdash$ Osp	(cAmEstrOp)	
$\therefore$ S es P	$\therefore$ Zsp			

IV.ª figura	Modos subalternos ($X, Y, Z \in \{$ A, E, I, O $\}$)			
		$Xpm, Yms \vdash Zsp$		
P es M	Xpm	Apm, E$ms \vdash$ Osp	(cAmEnOp)	
M es S	Yms			
$\therefore$ S es P	$\therefore$ Zsp			

donde, en todos ellos, A, E, I, O denotan las clases de proposiciones categóricas estudiadas en § 0.4.3 (pág. 35 de esta edición), correspondiendo la primera vocal a la premisa mayor, la segunda a la menor y la tercera a la conclusión; las consonantes cifran la manera de proceder para reducir cualquier modo de figuras distintas a la primera (modos imperfectos, según ARISTÓTELES) a modos de la primera (modos perfectos)[2].

Nos bastará con comprobar la validez de cualquiera de estos modos utilizando diagramas de VENN[3]. Por ejemplo, la figura 5.0 (pág. 403 de esta edición) pone de manifiesto la validez de Datisi.

Fijémonos ahora en Darapti —*cfr. infra* figura 5.1 (pág. 403 de esta edición)—. En este caso, no tenemos información sobre la existencia de entidades en la zona de intersección de S y P. Si pudiésemos asegurar que el término M no es vacío, que existiese alguna entidad que pudiese catalogarse

[2] *Cfr. v. gr.* GARRIDO [64] (págs. 160–161, nota al pie n.º 17).

[3] En un diagrama de VENN, una zona rayada indica que no existe ninguna entidad en ella, una zona con una cruz que existe alguna entidad en ella y una zona sin rayar y sin cruz que no existe información respecto a la existencia de entidades en la zona.

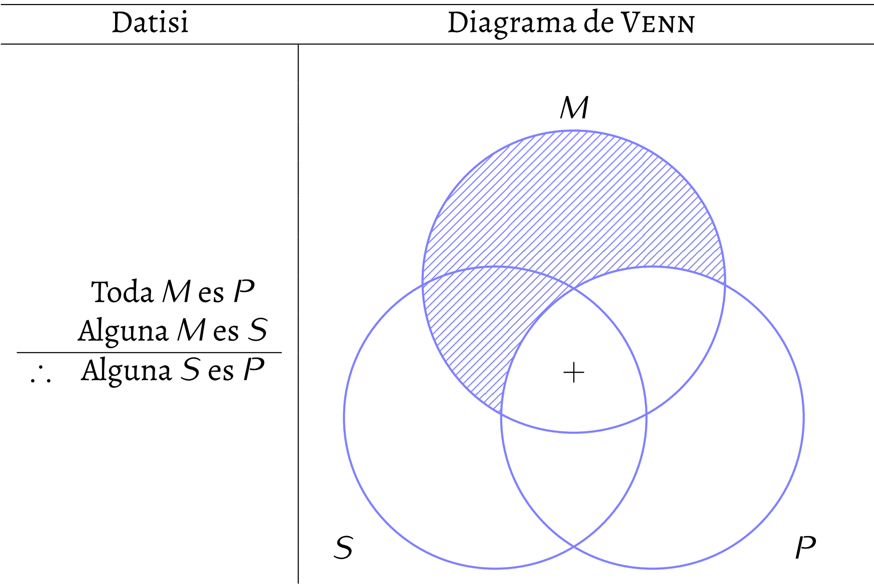


Figura 5.0.— Validez de dAtIsI mediante diagramas de Venn.

como perteneciente a M, entonces sí que la zona de intersección de S y P estaría marcada con una cruz. De hecho, Aristóteles suponía que todos los términos eran no vacíos. En la actualidad, no se supone necesariamente; es por esto por lo que en varios textos actuales encontramos que consideran Darapti un modo inválido.

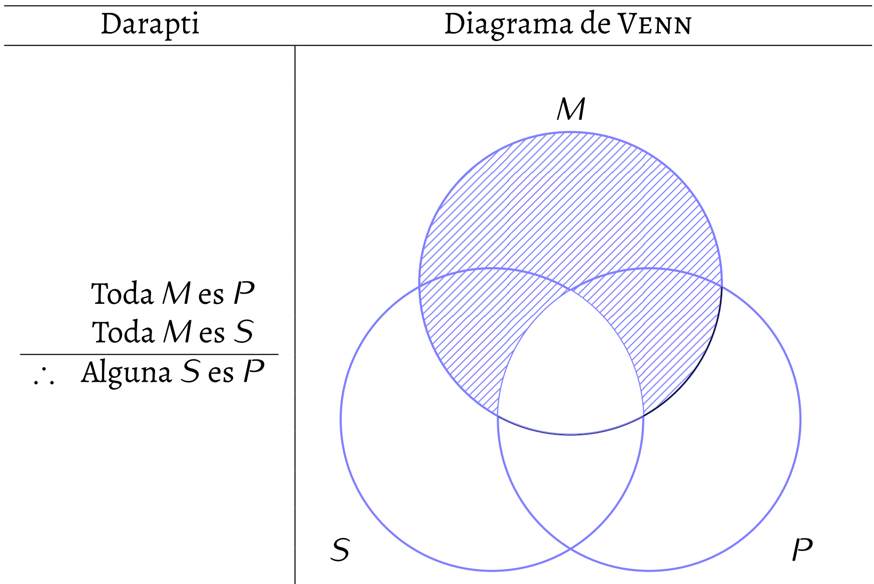


Figura 5.1.— No validez de dArAptI mediante diagramas de Venn.

De interesar una sistematización moderna de la silogística, concretamente la propuesta de Łukasiewicz de 1929, puede estudiarse en Garrido [64] (págs. 165–175).

§ 5.0.1 Silogismo hipotético

Definición 5.1.— Un *silogismo hipotético* (o, sinónimamente, *silogismo condicional*) es aquél cuya premisa mayor es una proposición condicional.

Este silogismo adopta dos figuras legítimas: *ponendo ponens* y *tollendo tollens*.

Ponendo ponens.

	Si Cris es una persona, es un ser con corazón.
	Cris es una persona.
∴	Cris es un ser con corazón.

Como vemos, se afirma la condición («Cris es una persona») en la premisa menor y lo condicionado («Cris es un ser con corazón») en la conclusión.

Puede ser vista como modo dArII de la I.ª figura del silogismo, concretando el término singular $s =$ Cris:

	M es P		Toda persona es un ser con corazón.
	s es M		Alguien (Cris) es una persona.
∴	s es P	∴	Alguien (Cris) es un ser con corazón.

Tollendo tollens.

	Si Cris es una persona, es un ser con corazón.
	Cris no es un ser con corazón.
∴	Cris no es una persona.

Como vemos, se niega lo condicionado («ser un ser con corazón») en la premisa menor y se niega la condición («ser una persona») en la conclusión.

Puede ser vista como modo bArOcO de la II.ª figura del silogismo, concretando el término singular $s =$ Cris:

	P es M		Toda persona es un ser con corazón.
	s no es M		Alguien (Cris) no es un ser con corazón.
∴	s no es P	∴	Alguien (Cris) no es una persona.

Observación 5.0.0.— No son legítimas las otras dos figuras posibles.

0. De afirmar la proposición condicionada no se sigue ni la afirmación ni la negación de la proposición condicionante; en el ejemplo:

	Si Cris es una persona, es un ser con corazón.
	Cris es un ser con corazón.
∴	¿Es Cris una persona?

De hecho, si optamos por el punto de vista de las figuras del silogismo categórico, debido a la función desempeñada por el término medio («ser con corazón») correspondería a la II.ª figura,

con premisa mayor universal afirmativa (A) y premisa menor particular afirmativa (I), modo que no es válido.

1. De negar la proposición condicionante no se sigue ni la afirmación ni la negación de la proposición condicionada; en el ejemplo:

	Si Cris es una persona, es un ser con corazón.
	Cris no es una persona.
∴	¿Es Cris un ser con corazón?

En esta ocasión, si optamos por el punto de vista de las figuras del silogismo categórico, debido a la función desempeñada por el término medio («ser persona») correspondería a la I.ª figura, con premisa mayor universal afirmativa (A) y premisa menor particular negativa (I), modo que no es válido.

§ 5.0.2 Silogismo disyuntivo y contravalente

Definición 5.2.— Un *silogismo disyuntivo* es aquél cuya premisa mayor es una disyunción de proposiciones.

Este silogismo adopta una figura legítima: *tollendo ponens*.

Tollendo ponens.

	Cris es una persona o es un robot.
	Cris no es un robot.
∴	Cris es una persona.

Como vemos, se niega un término de la disyunción («ser un robot») en la premisa menor y se afirma el otro («ser una persona») en la conclusión.

Definición 5.3.— Un *silogismo contravalente* es aquél cuya premisa mayor es una contravalencia de proposiciones.

El silogismo contravalente adopta dos figuras legítimas: *tollendo ponens* y *ponendo tollens*.

Ponendo tollens.

	Cris es una persona o es un robot.
	Cris es una persona.
∴	Cris no es un robot.

Como vemos, se afirma un término de la contravalencia («ser una persona») en la premisa menor y se niega el otro («ser un robot») en la conclusión.

Observación 5.0.1.— Debemos observar que la deducción disyuntiva y las deducciones contravalentes pueden ser vistas como deducciones condicionales. De esta manera, *tollendo ponens* puede

ser vista como *tollendo tollens*:

	Si Cris es una persona, no es un robot.
	No es cierto que Cris no sea un robot.
$\therefore$	No es cierto que Cris sea una persona.

y *ponendo tollens* puede ser vista como *ponendo ponens*:

	Si Cris es una persona, no es un robot.
	Cris es una persona.
$\therefore$	Cris no es un robot.

§ 5.0.3 Entimema

Definición 5.4.— Un *entimema* es un silogismo en el que se ha suprimido alguna premisa o la conclusión. Si no aparece la premisa mayor, decimos que es un *entimema de primer orden*, mientras que si la que no aparece es la menor, decimos que se trata de un *entimema de segundo orden*.

Ejemplo 200

Demostremos que el argumento

	Cris es una persona.
$\therefore$	Cris no es un robot.

es un entimema de primer orden.

Resolución.— En efecto, dicho argumento es un entimema de primer orden, ya que puede ser visto como modo fErIO de la I.ª figura del silogismo, concretando el sujeto $M =$ persona, el término singular $s =$ Cris y el predicado $P =$ ser robot,

M es P	Emp	Ninguna persona es un robot.
s es M	Ism	Alguien (Cris) es una persona.
$\therefore$ s es P	$\therefore$ Osp	$\therefore$ Alguien (Cris) no es un robot (es un no-robot).

en el que se ha suprimido la premisa mayor. ■

§ 5.1 La ley de Leibniz y la *reductio ad absurdum*

Leibniz introduce el concepto de igualdad en lógica basándose en el concepto de identidad[4], de ser lo mismo, «x es y» e «y es x», en el sentido de ocurrir que «cualquier x es y» y «cualquier y es x»

[4] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Principio_de_identidad.

—dos entidades son idénticas si, y sólo si, todo cuanto puede afirmarse de una puede afirmarse de la otra[5]—, se conoce como «ley de Leibniz» y puede formularse en lógica de segundo orden[6]:

$$\forall x\, \forall y\, [x = y \leftrightarrow \forall F\, (Fx \leftrightarrow Fy)]$$

No obstante, suelen distinguirse ambas implicaciones:

$$\forall x\, \forall y\, [x = y \rightarrow \forall F\, (Fx \leftrightarrow Fy)] \qquad \text{(indiscernibilidad de los idénticos)} \qquad (5.0)$$

$$\forall x\, \forall y\, [\forall F\, (Fx \leftrightarrow Fy) \rightarrow x = y] \qquad \text{(identidad de los indiscernibles)} \qquad (5.1)$$

existiendo controversia sobre la segunda[7].

Si x es idéntico a y, la indiscernibilidad de los idénticos significa que puede sustituirse uno por el otro en cualquier enunciado sin que cambie ninguna de las características cuantitativas ni cualitativas de éste.

Con los siguientes principios, Leibniz propone una lógica en la que puede demostrarse la de Aristóteles, en particular, cualquier silogismo.

- *Principio de identidad*: toda proposición se identifica consigo misma, es decir, se satisface

  $$\text{sea cual sea } x,\ x = x$$

  (también, equivalentemente, sea cual sea x, si x, entonces x);

- *Principio de sustitución*:

  $$\text{si } x \text{ es } y \text{ e } y \text{ es } z, \text{ entonces } x \text{ es } z$$

  (como dijimos antes, se afirma s es t con el sentido de que cualquier s es t);

- *Principio de la no contradicción*: ninguna proposición puede ser afirmada y negada simultáneamente, es decir, se satisface

  $$\text{no } (p \text{ y no } p);$$

- *Principio del tercio excluso*: toda proposición es afirmada o negada, sin existir una tercera posibilidad, es decir, se satisface

  $$p \text{ o no } p.$$

[5] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Identidad_de_los_indiscernibles y https://plato.stanford.edu/archives/fall2008/entries/identity-indiscernible/.

[6] *Vid. supra* pág. 372.

[7] *Cfr. v. gr.* Max Black [102].

La *lógica ecuacional*[8] hunde sus raíces en esta propuesta, pero también la *lógica algebraica*[9]: el álgebra de conceptos (1690) de LEIBNIZ (equivalente al álgebra de BOOLE [1847-1853]) y su metafísica son de importancia en *metafísica computacional*, en *razonamiento automático*.

Observemos que admitidos el principio de la no contradicción, $\neg(p\wedge\neg p)$ y el principio del tercio excluso, $p \vee \neg p$, se deduce que, o bien p, o bien $\neg p$, esto es, en notación actual, $p \veebar \neg p$. Es decir, de ambos principios se deduce,

0. que un enunciado es falso cuando no es verdadero, $(\neg x) = \neg(x)$, y
1. que un enunciado es verdadero cuando no es falso, $(x) = \neg(\neg x)$.

En realidad, el principio del tercio excluso puede ser reformulado como $p \leftrightarrow \neg\neg p$.

De (0), y de que una contradicción es un enunciado que nunca es verdadero, se deduce el método de demostración de la *reductio ad absurdum*: todo enunciado del que se deduzca una contradicción es falso[10] y, por tanto, por el principio del tercio excluso, la negación de tal enunciado es verdadero.

§ 5.2 Deducción formal y sistemas deductivos

Lo estudiado en § 2.0 (pág. 177 de esta edición) y en § 2.1 (pág. 184 de esta edición) es de aplicación en la lógica de cuantores.

§ 5.3 Sistema de deducción natural para la cuantificación monádica

De igual modo que como hacíamos en lógica de juntores[11], consideramos unas reglas básicas, a partir de las cuales somos capaces de generar todos los teoremas de la lógica de primer orden. La presente exposición se fundamenta en el *sistema de deducción natural* (SDN), elaborado independientemente por GENTZEN [80] (1935) y JAŚKOWSKI [81] (1934).

Comenzamos con el SDN para la cuantificación monádica (LPO-M).

§ 5.3.0 Reglas deductivas básicas

Vemos a continuación las *reglas de inferencia deductivas básicas* del SDN para la LPO-M.

[8] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Equational_logic.
[9] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Algebraic_logic.
[10] Por un lado, afirmar que el enunciado x es $\perp$ (una contradicción) es afirmar que x es falso, por otro, el fundamento de la secuencia presente en una deducción es el principio de sustitución: x es y e y es $\perp$, entonces x es $\perp$, aplicado tantas veces como sea necesario.
[11] *Vid.* § 2.2 (pág. 190 de esta edición).

Regla de introducción del generalizador (IG)

$$\frac{Pa}{\forall x Px}$$

Tengamos presente que a no es una constante, una entidad concreta del dominio, sino todo lo contrario, a representa una entidad cualquiera, libre de cualquier condición. Por ejemplo, si de $Pa \vee Qa$ deducimos Pa, esto es una suposición, luego no es admisible aplicar la regla para obtener $\forall x Px$. Esta regla refleja la idea de representante de una clase, entendiendo por tal, a una entidad que goza de todas las propiedades comunes de las entidades de la clase, en el sentido de que si una afirmación es demostrada para ella, no hace falta demostrarla para el resto de entidades de la clase.

Regla de eliminación del generalizador (EG)

$$\frac{\forall x Px}{Pa}$$

Regla de introducción del particularizador (IP)

$$\frac{Pa}{\exists x Px}$$

Regla de eliminación del particularizador (EP)

$$\begin{array}{l} \exists x Px \\ \left| \begin{array}{l} Pa \\ \vdots \\ A \end{array} \right. \\ \hline A \end{array}$$

Debemos tener en cuenta que a representa una entidad que si bien verifica P, no debe poseer ninguna otra propiedad, esto es, no debe haber intervenido en pasos anteriores de la demostración. Además no debe aparecer en A. Esta regla representa la idea de que si sabemos que existe una entidad y de la existencia de esa entidad deducimos una conclusión, entonces no hace falta identificar a tal entidad para tener la conclusión. Por ejemplo, de

$$\exists x Px \leftrightharpoons \text{ hay una sustancia resbaladiza en el suelo,}$$

concluimos

$$A \leftrightharpoons \text{ es posible que nos caigamos si no vamos con cuidado,}$$

sin tener que identificar la sustancia, ya sea aceite, una cáscara de plátano, etc.

Ejemplo 201

Resolvamos la siguiente argumentación.

Un paquete de este segmento de red no ha sido escaneado por el antivirus. Todos los paquetes de este segmento de red fueron validados por el cortafuegos. Por lo tanto, algún paquete validado por el cortafuegos no ha sido escaneado por el antivirus.

Resolución.— Su formalización en lógica de primer orden es:

Sx	x es un paquete de este segmento de red,
Ax	x ha sido escaneado por el antivirus,
Cx	x ha sido validado por el cortafuegos,

con el esquema argumental

$$\{\exists x(Sx \land \neg Ax), \forall x(Sx \to Cx)\} \vdash \exists x(Cx \land \neg Ax),$$

que en el lenguaje de la lógica de primer orden queda la expresión

$$\exists x(Sx \land \neg Ax) \land \forall x(Sx \to Cx) \to \exists x(Cx \land \neg Ax).$$

Una deducción formal que demuestra la validez de la argumentación es la siguiente:

0.	$\exists x(Sx \land \neg Ax)$	Premisa
1.	$\forall x(Sx \to Cx)$	Premisa
2.	$Sa \land \neg Aa$	EP 0
3.	Sa	EC 2
4.	$\neg Aa$	EC 2
5.	$Sa \to Ca$	EG 1
6.	Ca	MP 3,5
7.	$Ca \land \neg Aa$	IC 6,4
8.	$\exists x(Cx \land \neg Ax)$	IP 7



§ 5.3.1 Reglas deductivas derivadas

Reglas de interdefinición

Teorema 5.0 (RD de interdefinición de ∀ y ∃)

Definición del generalizador (DG): $\dfrac{\forall x Px}{\neg\exists x \neg Px}$ (doble línea)

Definición del particularizador (DP) $\dfrac{\exists x Px}{\neg\forall x \neg Px}$ (doble línea)

Negación del generalizador (NG) $\dfrac{\neg\forall x Px}{\exists x \neg Px}$ (doble línea)

Negación del particularizador (NP) $\dfrac{\neg\exists x Px}{\forall x \neg Px}$ (doble línea)

Reglas de descenso y de mutación

Teorema 5.1 (RD de descenso)

Descenso (Desc): $\dfrac{\forall x Px}{\exists x Px}$

Teorema 5.2 (RD de mutación de variable ligada)

Mutación en el generalizador (MVG): $\dfrac{\forall x Px}{\forall y Py}$ (doble línea)

Mutación en el particularizador (MVP) $\dfrac{\exists x Px}{\exists y Py}$ (doble línea)

Reglas de distribución

Teorema 5.3 (RD de distribución de ∀ y ∃ en ∧)

Distribución de de ∀ en ∧ (DGC): $$\frac{\forall x\,(Px \wedge Qx)}{\forall x Px \wedge \forall x Qx}$$ (doble línea)

Distribución de ∃ en ∧ (DPC_0) $$\frac{\exists x\,(Px \wedge Qx)}{\exists x Px \wedge \exists x Qx}$$

Distribución de ∃ en ∧ (DPC_1) $$\frac{\exists x Px \wedge \forall x Qx}{\exists x\,(Px \wedge Qx)}$$

Teorema 5.4 (RD de distribución de ∀ y ∃ en ∨)

Distribución de ∃ en ∨ (DPD): $$\frac{\exists x\,(Px \vee Qx)}{\exists x Px \vee \exists x Qx}$$ (doble línea)

Distribución de ∀ en ∨ (DGD_0) $$\frac{\forall x Px \vee \forall x Qx}{\forall x\,(Px \vee Qx)}$$

Distribución de ∀ en ∨ (DGD_1) $$\frac{\forall x\,(Px \vee Qx)}{\forall x Px \vee \exists x Qx}$$

Teorema 5.5 (RD de distribución de ∀ y ∃ en →)

Distribución de de ∀ en → (DGI_0): $$\frac{\forall x\,(Px \rightarrow Qx)}{\forall x Px \rightarrow \forall x Qx}$$

Distribución de de ∀ en → (DGI_1): $$\frac{\forall x\,(Px \rightarrow Qx)}{\exists x Px \rightarrow \exists x Qx}$$

Distribución de ∃ en → (DPI_0): $$\frac{\exists x\,(Px \rightarrow Qx)}{\forall x Px \rightarrow \exists x Qx}$$

Distribución de ∃ en → (DPI_1): $$\frac{\exists x Px \rightarrow \exists x Qx}{\exists x\,(Px \rightarrow Qx)}$$

Teorema 5.6 (RD de distribución de ∀ y ∃ en ↔)

Distribución de ∀ en ↔ (DGCo$_0$): $\dfrac{\forall x\,(Px \leftrightarrow Qx)}{\forall x Px \leftrightarrow \forall x Qx}$

Distribución de ∀ en ↔ (DGCo$_1$) $\dfrac{\forall x\,(Px \leftrightarrow Qx)}{\exists x Px \leftrightarrow \exists x Qx}$

Reglas de distribución condicionales

Empleamos la denominación adoptada por Manuel Garrido [64] (pág. 184) para estas reglas. La condición a la que están sujetas es a que x esté ligada en A.

Teorema 5.7 (RD de distribución condicional de ∀ y ∃ en ∧)

Distribución condicional de ∀ en ∧ (DistC$_0$): $\dfrac{A \wedge \forall x Px}{\forall x\,(A \wedge Px)}$ (doble línea)

Distribución condicional de ∃ en ∧ (DistC$_1$): $\dfrac{A \wedge \exists x Px}{\exists x\,(A \wedge Px)}$ (doble línea)

Teorema 5.8 (RD de distribución condicional de ∀ y ∃ en ∨)

Distribución condicional de ∀ en ∨ (DistD$_0$): $\dfrac{A \vee \forall x Px}{\forall x\,(A \vee Px)}$ (doble línea)

Distribución condicional de ∃ en ∨ (DistD$_1$): $\dfrac{A \vee \exists x Px}{\exists x\,(A \vee Px)}$ (doble línea)

Teorema 5.9 (RD de distribución condicional de ∀ en →)

Distribución condicional de ∀ en → (DistGI$_0$): $\dfrac{\forall x\,(A \rightarrow Px)}{(A \rightarrow \forall x Px)}$ (doble línea)

Distribución condicional de ∀ en → (DistGI$_1$): $\dfrac{\forall x\,(Px \rightarrow A)}{(\exists x Px \rightarrow A)}$ (doble línea)

Teorema 5.10 (RD de distribución condicional de ∃ en →)

Distribución condicional de ∃ en → (DistPI_0):
$$\frac{\exists x\,(A \to Px)}{(A \to \exists x Px)}$$

Distribución condicional de ∃ en → (DistPI_1):
$$\frac{\exists x\,(Px \to A)}{(\forall x Px \to A)}$$

Una muestra de por qué no basta con la lógica de juntores y se hace necesaria la lógica de cuantores —y por ende, la lógica de primer orden (la reunión de ambas)—, nos la proporciona el siguiente ejemplo.

Ejemplo 202

Resolvamos la siguiente argumentación.

> No hay personas malas entre las defensoras de esta causa. Ninguna persona buena miente. Todas mis amistades defienden esta causa. Luego mis amistades no mienten.

[Cubit 41]. *Cfr.* Deaño [103]: págs. 170–171.

Resolución.— En el ámbito de la lógica de juntores, no estamos ante una argumentación válida, al ser contingente, pues dicha argumentación se formaliza como:

p	no hay personas malas entre las defensoras de esta causa,
q	ninguna persona buena miente,
r	todas mis amistades defienden esta causa,
s	mis amistades no mienten,

con el esquema argumental

$$\{p, q, r\} \vdash s.$$

Sin embargo, sí que se trata de una argumentación válida. Pero, para demostrarlo necesitamos de la lógica de primer orden. Su formalización en esta lógica es

Mx	x es una persona mala,
Cx	x defiende esta causa,
Nx	x miente,
Ax	x es una de mis amistades,

con el esquema argumental

$$\{\neg\exists x(Mx \wedge Cx), \forall x(\neg Mx \to \neg Nx), \forall x(Ax \to Cx)\} \vdash \forall x(Ax \to \neg Nx),$$

que en el lenguaje de la lógica de primer orden queda la expresión

$$(\neg\exists x(Mx \wedge Cx) \wedge \forall x(\neg Mx \to \neg Nx) \wedge \forall x(Ax \to Cx)) \to \forall x(Ax \to \neg Nx).$$

Una deducción formal que demuestra la validez de la argumentación es la siguiente:

0.	$\neg\exists x(Mx \wedge Cx)$	Premisa
1.	$\forall x(\neg Mx \to \neg Nx)$	Premisa
2.	$\forall x(Ax \to Cx)$	Premisa
3.	$\neg\exists x(Mx \wedge Cx) \wedge \forall x(\neg Mx \to \neg Nx)$	IC 0, 1
4.	$\neg\exists x(Mx \wedge Cx) \wedge \forall x(\neg Mx \to \neg Nx) \wedge \forall x(Ax \to Cx)$	IC 3, 2
5.	$\forall x\neg(Mx \wedge Cx)$	NP 0
6.	$\forall x(\neg Mx \vee \neg Cx)$	DM_1 5
7.	$\forall x(Mx \to \neg Cx)$	DI_0 6
8.	$Ma \to \neg Ca$	EG 7
9.	$\neg Ma \to \neg Na$	EG 1
10.	$Aa \to Ca$	EG 2
11.	$Ca \to \neg Ma$	Cp_1 8
12.	$Aa \to \neg Ma$	Sil 10, 11
13.	$Aa \to \neg Na$	Sil 12, 9
14.	$\forall x(Ax \to \neg Nx)$	IG 13
15.	$(\neg\exists x(Mx \wedge Cx) \wedge \forall x(\neg Mx \to \neg Nx) \wedge \forall x(Ax \to Cx)) \to \forall x(Ax \to \neg Nx)$	II 4–14

donde:

NP es la regla (doble) de negación del particularizador $\neg\exists xPx \dashv\vdash \forall x\neg Px$;

DI_0 es la regla (doble) definición del implicador (principio de FILÓN) $\phi \to \psi \dashv\vdash \neg\phi \vee \psi$;

Cp_1 es la ley de contraposición $\phi \to \neg\psi \vdash \psi \to \neg\phi$;

Sil es la ley del silogismo hipotético $\{\phi \to \psi, \psi \to \chi\} \vdash \phi \to \chi$;

II es la introducción del implicador (el teorema de la deducción [TD]). 

Ejemplo 203

En un monte hay 77 animales, los cuales tienen o dos o cuatro patas. Una persona del lugar le dice: «Al menos uno de los animales tiene dos patas, y dado cualquier par de animales, al menos uno de los dos tiene cuatro patas».

a. Formalicemos en el lenguaje de la lógica de cuantores esto que nos han dicho.
b. ¿Cuántos animales hay de dos y de cuatro patas?

[Cubit 42].

Resolución.— Considerando como universo de discurso el conjunto de los animales en dicho monte, sean:

$$Dx \risingdotseq x \text{ tiene dos patas,}$$
$$Cx \risingdotseq x \text{ tiene cuatro patas.}$$

a. $\exists x Dx \land \forall xy\,(Cx \lor Cy)$;

b.

Paso	*Razón*
0. $\exists x Dx$	Premisa
1. $\forall xy\,(Cx \lor Cy)$	Premisa
2. $Ca \lor Cb$	EG 1 (eliminacion del generalizador)
3. $\forall x\,(Cx \leftrightarrow \neg Dx)$	Premisa
4. $Ca \leftrightarrow \neg Da$	EG 3 (eliminacion del generalizador)
5. $Ca \to \neg Da$	ECO_1 4 (eliminacion del coimplicador)
6. $Cb \leftrightarrow \neg Db$	EG 3 (eliminacion del generalizador)
7. $Cb \to \neg Db$	ECO_1 6 (eliminacion del coimplicador)
8. $\neg Da \lor \neg Db$	Dil_3 2, 5, 7 (dilema constructivo complejo*)
9. $\neg\,(Da \land Db)$	DM_1 8 (ley de De Morgan de negacion del conjuntor)
10. $\forall x \forall y \neg\,(Dx \land Dy)$	IG^2 9 (introduccion multiple del generalizador)
11. $\forall y \neg\,(Da \land Dy)$	EG 10 (eliminacion del generalizador)
12. $\neg \exists y\,(Da \land Dy)$	NP 11 (negacion del particularizador)
13. $\forall x \neg \exists y\,(Dx \land Dy)$	IG 12 (introduccion del generalizador)
14. $\neg \exists x \exists y\,(Dx \land Dy)$	NP 13 (negacion del particularizador)

* Dilema constructivo complejo: $(\phi \to \chi) \land (\psi \to \tau) \to (\phi \lor \psi \to \chi \lor \tau)$ (*cfr. supra* actividad 3.8 [pág. 338 de esta edición]).

La traducción de (0) y (14) al español es: (0) existe un animal de dos patas y (14) no existe ninguna pareja en la que ambos tengan dos patas. Esto implica que sólo hay un animal de dos patas y, por tanto, 76 de cuatro patas. ■

Ejemplo 204

Traducido de: Lewis Carroll, *Symbolic Logic: Part I*. Elementary (Macmillan, 1896), pág. 118. Dominio Público.

I. Ningún gatito que gusta del pescado es indomesticable;
II. Ningún gatito sin cola jugará con un gorila;
III. A los gatitos con bigotes les gusta el pescado;
IV. Ningún gatito domesticable tiene ojos verdes;
V. Ningún gatito tiene cola a menos que tenga bigotes.

Universo = «gatitos»; A = gusta del pescado; B = ojos verdes; C = con cola; D = domesticable; E = con bigotes; H = jugará con un gorila.

Debemos:

a. Formalizar en lógica de cuantores todas estas afirmaciones.
b. En el universo de los gatitos y usando lógica de cuantores, deducir la única conclusión que se sigue de estas afirmaciones y que hace que el argumento sea válido.
c. Traducir nuestra respuesta simbólica a español.

[Cubit 43].

Resolución.— Considerando como universo de discurso el conjunto de los gatitos, sean, pues:

$$Dx \leftarrow \text{«}x \text{ es domesticable»},$$
$$Ax \leftarrow \text{«}x \text{ gusta del pescado»},$$
$$Cx \leftarrow \text{«}x \text{ tiene cola»},$$
$$Hx \leftarrow \text{«}x \text{ juega con un gorila»},$$
$$Ex \leftarrow \text{«}x \text{ tiene bigotes»},$$
$$Bx \leftarrow \text{«}x \text{ tiene ojos verdes»}.$$

a. I. $\forall x(\neg Dx \to \neg Ax)$;

II. $\forall x(\neg Cx \to \neg Hx)$;

III. $\forall x(Ex \to Ax)$;

IV. $\forall x(Dx \to \neg Bx)$;

V. $\forall x(\neg Ex \to \neg Cx)$.

b.

Paso	*Razón*
0. $\forall x(\neg Dx \rightarrow \neg Ax)$	Premisa
1. $\forall x(\neg Cx \rightarrow \neg Hx)$	Premisa
2. $\forall x(Ex \rightarrow Ax)$	Premisa
3. $\forall x(Dx \rightarrow \neg Bx)$	Premisa
4. $\forall x(\neg Ex \rightarrow \neg Cx)$	Premisa
5. $\neg Da \rightarrow \neg Aa$	EG 0 (eliminacion del generalizador)
6. $\neg Ca \rightarrow \neg Ha$	EG 1 (eliminacion del generalizador)
7. $Ea \rightarrow Aa$	EG 2 (eliminacion del generalizador)
8. $Da \rightarrow \neg Ba$	EG 3 (eliminacion del generalizador)
9. $\neg Ea \rightarrow \neg Ca$	EG 4 (eliminacion del generalizador)
10. $\neg Aa \rightarrow \neg Ea$	Cp_1 7 (ley de contraposicion)
11. $Ba \rightarrow \neg Da$	Cp_2 8 (ley de contraposicion)
12. $(Ba \rightarrow \neg Da) \wedge (\neg Da \rightarrow \neg Aa)$	IC 11, 5 (introduccion de la conjuncion)
13. $(Ba \rightarrow \neg Aa)$	Sil 12 (ley del silogismo hipotetico)
14. $(Ba \rightarrow \neg Aa) \wedge (\neg Aa \rightarrow \neg Ea)$	IC 13, 10 (introduccion de la conjuncion)
15. $(Ba \rightarrow \neg Ea)$	Sil 14 (ley del silogismo hipotetico)
16. $(Ba \rightarrow \neg Ea) \wedge (\neg Ea \rightarrow \neg Ca)$	IC 15, 9 (introduccion de la conjuncion)
17. $(Ba \rightarrow \neg Ca)$	Sil 16 (ley del silogismo hipotetico)
18. $(Ba \rightarrow \neg Ca) \wedge (\neg Ca \rightarrow \neg Ha)$	IC 17, 6 (introduccion de la conjuncion)
19. $(Ba \rightarrow \neg Ha)$	Sil 18 (ley del silogismo hipotetico)
20 $\forall x(Bx \rightarrow \neg Hx)$	IG 19 (introduccion del generalizador)

c. Ningún gatito de ojos verdes jugará con un gorila. ■

§ 5.4 Sistema de deducción natural para la cuantificación poliádica

§ 5.4.0 Reglas deductivas básicas

Vemos a continuación las *reglas de inferencia deductivas básicas* del SDN para la LPO-P.

Simplificamos la notación de los cuantores múltiples al máximo. Por ejemplo, $\forall x_0 \ldots x_{n-1}$, que también pudiésemos notar $\forall^n x_0 \ldots x_{n-1}$, es una abreviatura de $\forall x_0 \forall x_1 \ldots \forall x_{n-1}$.

Regla de introducción del generalizador (IG^n)

$$\frac{Pa_0 \ldots a_{n-1}}{\forall x_0 \ldots x_{n-1} P x_0 \ldots x_{n-1}}$$

Regla de eliminación del generalizador (EG^n)

$$\frac{\forall x_0 \dots x_{n-1} P x_0 \dots x_{n-1}}{P a_0 \dots a_{n-1}}$$

Regla de introducción del particularizador (IP^n)

$$\frac{P a_0 \dots a_{n-1}}{\exists x_0 \dots x_{n-1} P x_0 \dots x_{n-1}}$$

Regla de eliminación del particularizador (EP^n)

$$\begin{array}{l} \exists x_0 \dots x_{n-1} P x_0 \dots x_{n-1} \\ \left| \begin{array}{l} P a_0 \dots a_{n-1} \\ \vdots \\ A \end{array} \right. \\ \hline A \end{array}$$

Las consideraciones hechas en cuantificación monádica para las reglas IG y EP son válidas para las reglas IG^n y EP^n, sólo que aquí debemos hacerlo extensivo a todos los parámetros.

§ 5.4.1 Reglas deductivas derivadas

Teorema 5.11 (RD conmutativas de ∀ y ∃ en cuantificación diádica)

Conmutativa del generalizador (CoG²):
$$\frac{\forall x \forall y P x y}{\overline{\forall y \forall x P x y}}$$

Conmutativa del particularizador (CoP²)
$$\frac{\exists x \exists y P x y}{\overline{\exists y \exists x P x y}}$$

Teorema 5.12 (RD de conmutación de ∃ y ∀ en cuantificación diádica)

Conmutación de ∃ y ∀ (ComPG):
$$\frac{\exists x \forall y P x y}{\forall y \exists x P x y}$$

Teorema 5.13 (RD de reducción del ∀ en cuantificación diádica)

Reducción de ∀ (RedG^2):
$$\frac{\forall x \forall y Pxy}{\forall x Pxx}$$

Teorema 5.14 (RD de duplicación del ∃ en cuantificación diádica)

Duplicación del ∃ (DupP^2):
$$\frac{\exists x Pxx}{\exists x \exists y Pxy}$$

Las reglas CoG^2, CoP^2, RedG^2 y DupP^2 se generalizan a la cuantificación poliádica.

Teorema 5.15 (RD CoG^n, CoP^n, RedG^n y DupP^n)

Conmutativa del generalizador (CoG^n):
$$\frac{\forall x_0 \dots x_{n-1} P x_0 \dots x_{n-1}}{\forall x_{\sigma(0)} \dots x_{\sigma(n-1)} P x_0 \dots x_{n-1}}$$

Conmutativa del particularizador (CoP^n):
$$\frac{\exists x_0 \dots x_{n-1} P x_0 \dots x_{n-1}}{\exists x_{\sigma(0)} \dots x_{\sigma(n-1)} P x_0 \dots x_{n-1}}$$

Reducción de ∀ (RedG^n):
$$\frac{\forall x_0 \dots x_{n-1} P x_0 \dots x_{n-1}}{\forall x_k P x_k \dots x_k}$$

Duplicación del ∃ (DupP^n):
$$\frac{\exists x_k P x_k \dots x_k}{\exists x_0 \dots x_{n-1} P x_0 \dots x_{n-1}}$$

donde σ es una permutación de $\{0, \dots, n-1\}$ y $k \in \{0, \dots, n-1\}$.

Actividad 5.1

Demostremos la regla de descenso cuantorial para cuantificación poliádica (Desc^n):
$$\frac{\forall x_0 \dots x_{n-1} P x_0 \dots x_{n-1}}{\exists x_0 \dots x_{n-1} P x_0 \dots x_{n-1}}$$

§ 5.5 Normalización: forma normal prenexa (FNP)

Definición 5.5.— Decimos que una fórmula A está en *forma normal prenexa* (FNP) si, y sólo si, en ella sólo aparecen juntores de la base $\{\neg, \wedge, \vee\}$ y todos los cuantores están situados al principio de A (en otras palabras, su matriz lógica no contiene cuantores).

Aunque su exposición es desde la sintaxis, lo que establecemos tiene una expresión inmediata en la semántica como una estrategia de deducción semántica más. Este desarrollo indistinto en la sintaxis y en la semántica sucede porque la lógica de primer orden es consistente y completa[12].

Caso de presentar la forma normal prenexa desde la semántica, entonces, en el teorema 5.16 (pág. 422 de esta edición), las reglas de inferencia deductivas dobles (⊣⊢) serían sustituidas por equivalencias lógicas (⫤⊨), por lo que las reglas de inferencia deductivas simples serían sustituidas por implicaciones lógicas (⊨).

§ 5.5.0 Algoritmo de obtención de la forma normal prenexa de una fórmula dada

Si nuestro interés radica en encontrar la forma normal prenexa de una fórmula dada, entonces es oportuno aplicar el siguiente procedimiento, siempre teniendo presente que si en cualquier momento necesitásemos alguna otra equivalencia de las que aparecen a continuación, sería admisible utilizarla.

Suponemos que la fórmula está definida en las bases $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$ de juntores y $\{\exists, \forall\}$ de cuantores. Ahora bien, si participasen más juntores, en el paso FNP0 eliminaríamos todos los que no fuesen de la base $\{\neg, \vee, \wedge\}$.

Paso 0 (FNP0).
Eliminación de ↔ y →.

$$\begin{aligned} \text{CO}: &\quad A \leftrightarrow B \dashv\vdash (A \rightarrow B) \wedge (B \rightarrow A); \\ \text{DI}_0: &\quad A \rightarrow B \dashv\vdash \neg A \vee B \\ \text{DI}_1: &\quad A \rightarrow B \dashv\vdash \neg(A \wedge \neg B). \end{aligned}$$

Paso 1 (FNP1).
Interiorización de ¬.

$$\begin{aligned} \text{DN}: &\quad \neg\neg A \dashv\vdash A; \\ \text{DM}_0: &\quad \neg(A \vee B) \dashv\vdash \neg A \wedge \neg B; \\ \text{DM}_1: &\quad \neg(A \wedge B) \dashv\vdash \neg A \vee \neg B; \\ \text{NG}: &\quad \neg\forall x P x \dashv\vdash \exists x \neg P x; \\ \text{NP}: &\quad \neg\exists x P x \dashv\vdash \forall x \neg P x. \end{aligned}$$

Paso 2 (FNP2).
Exteriorización de todos los cuantores que afecten a conjunciones o disyunciones. Si x está libre en

[12] *Vid. infra* § 6.1.0 (pág. 452 de esta edición).

A, entonces mutar:

$$\begin{array}{rll} \text{MG}: & \forall x Px \dashv\vdash \forall y Py; & [\text{TI}] \\ \text{MP}: & \exists x Px \dashv\vdash \exists y Py. & [\text{TI}] \end{array}$$

Utilizar las reglas de distribución condicional de $\forall$ y $\exists$ en $\wedge$ y en $\vee$:

$$\begin{array}{rl} \text{DistC}_0: & A \wedge \forall x Px \dashv\vdash \forall x(A \wedge Px); \\ \text{DistC}_1: & A \wedge \exists x Px \dashv\vdash \exists x(A \wedge Px); \\ \text{DistD}_0: & A \vee \forall x Px \dashv\vdash \forall x(A \vee Px); \\ \text{DistD}_1: & A \vee \exists x Px \dashv\vdash \exists x(A \vee Px). \end{array}$$

Teorema 5.16 (Obtención de la forma normal prenexa de una fórmula)
Mediante el procedimiento anterior se obtiene la forma normal prenexa de una fórmula dada.

Ilustremos este procedimiento con el siguiente ejemplo.

Ejemplo 205

Obtengamos la FNP de $\exists x(Qx \wedge (\forall y Pxy \vee \neg\forall y Qy)) \to \forall x Rx$.

Resolución.— Hagamos una derivación formal.

0.	$\exists x(Qx \wedge (\forall y Pxy \vee \neg\forall y Qy)) \to \forall x Rx$	(fórmula)
1.	$\neg\exists x(Qx \wedge (\forall y Pxy \vee \neg\forall y Qy)) \vee \forall x Rx$	(DI 0) [FNP0]
2.	$\forall x\neg(Qx \wedge (\forall y Pxy \vee \neg\forall y Qy)) \vee \forall x Rx$	(NP 1) [FNP1]
3.	$\forall x\neg(Qx \wedge (\forall y Pxy \vee \exists y\neg Qy)) \vee \forall x Rx$	(NG 2) [FNP1]
4.	$\forall x(\neg Qx \vee \neg(\forall y Pxy \vee \exists y\neg Qy)) \vee \forall x Rx$	(DM_1 3) [FNP1]
5.	$\forall x(\neg Qx \vee (\neg\forall y Pxy \wedge \neg\exists y\neg Qy)) \vee \forall x Rx$	(DM_0 4) [FNP1]
6.	$\forall x(\neg Qx \vee (\exists y\neg Pxy \wedge \neg\exists y\neg Qy)) \vee \forall x Rx$	(NG 5) [FNP1]
7.	$\forall x(\neg Qx \vee (\exists y\neg Pxy \wedge \forall y\neg\neg Qy)) \vee \forall x Rx$	(NP 6) [FNP1]
8.	$\forall x(\neg Qx \vee (\exists y\neg Pxy \wedge \forall y Qy)) \vee \forall x Rx$	(DN 7) [FNP2]
9.	$\forall z(\neg Qz \vee (\exists y\neg Pzy \wedge \forall y Qy)) \vee \forall x Rx$	(MG 8) [FNP2]
10.	$\forall x\forall z(\neg Qz \vee (\exists y\neg Pzy \wedge \forall y Qy)) \vee Rx$	(DistD_0 9) [FNP2]
11.	$\forall x\forall z(\neg Qz \vee (\exists y\neg Pzy \wedge \forall w Qw)) \vee Rx$	(MG 10) [FNP2]

12. $\forall x \forall z(\neg Qz \vee \exists y(\neg Pzy \wedge \forall w Qw)) \vee Rx$ (DistC$_1$ 11) [FNP2]

13. $\forall x \forall z \exists y(\neg Qz \vee (\neg Pzy \wedge \forall w Qw)) \vee Rx$ (DistD$_1$ 12) [FNP2]

14. $\forall x \forall z \exists y(\neg Qz \vee \forall w(\neg Pzy \wedge Qw)) \vee Rx$ (DistC$_0$ 13) [FNP2]

15. $\forall x \forall z \exists y \forall w(\neg Qz \vee (\neg Pzy \wedge Qw)) \vee Rx$ (DistD$_0$ 14) [FNP2]

Solución.— La forma normal prenexa buscada es $\forall x \forall z \exists y \forall w((\neg Qz \vee (\neg Pzy \wedge Qw)) \vee Rx$. ■

§ 5.6 Variaciones de la lógica de primer orden

Vemos en este subcapítulo, sucintamente, tres extensiones de la lógica de primer orden. Aquí, empleamos el término extensiones en el sentido de Susan Haack [104], esto es, la colección de fórmulas (resp., teoremas/inferencias) de estas variaciones incluyen propiamente la colección de fórmulas (resp., teoremas/inferencias) de $\mathcal{L}_1$.

§ 5.6.0 Lógica y cálculo de primer orden con identidad

Añadiendo el signo «=» a $\mathcal{L}_1$ obtenemos un nuevo lenguaje que notamos por $\mathcal{L}_1^=$.

Dos detalles que debemos tener presente son: por una parte, si bien pudiésemos interpretar $=$ como un predicado, por ser una relación, observemos que en realidad es una *constante de predicado* ya que siempre es la misma relación; por otra, la notación habitual de los predicados es prefijo (notaríamos $= xy$) mientras que lo habitual es que la notación de la igualdad sea infijo, esto es, $x = y$.

A continuación presentamos el cálculo de identidad de Kalish y Montague.

Reglas básicas

Reglas básicas

Introducción de identidad (IId):

$$\frac{Pt}{(\forall x)(x = t \rightarrow Px)}$$

Eliminación de identidad (EId):

$$\frac{(\forall x)(x = t \rightarrow Px)}{Pt}$$

Interpretamos la regla IId como sigue: si afirmamos que el término t satisface el predicado P, entonces toda entidad que se identifique con t también satisface P.

Ejemplo 206

Resolvamos el siguiente argumento.

Lo que ha jaqueado el sistema es un bot. Uoeb es lo que ha jaqueado el sistema. Luego Uoeb es un bot.

Resolución.— Formalicemos; sean:

$t \fallingdotseq$ lo que ha jaqueado el sistema;

$b \fallingdotseq$ Uoeb;

$B \fallingdotseq$ ser un bot.

Resolvamos:

0.	Bt	Premisa
1.	$b = t$	Premisa
2.	$\forall x(x = t \to Bx)$	IId 0
3.	$b = t \to Bb$	EG 2
4.	Bb	MPP 3,1

Hemos demostrado que se trata de un argumento válido. ■

Interpretamos la regla EId como sigue: si afirmamos que toda entidad que se identifique con el término t satisface el predicado P, entonces el término t también satisface P.

Ejemplo 207

Resolvamos el siguiente argumento.

Toda réplica del sistema está jaqueada. Luego el sistema está jaqueado.

Resolución.— Formalicemos; sean:

$t \fallingdotseq$ el sistema;

$(x = t) \fallingdotseq x$ es una réplica de t;

$J \fallingdotseq$ estar jaqueado.

Resolvamos:

0.	$\forall x(x = t \to Jx)$	Premisa
1.	Jt	EId 0

Hemos demostrado que se trata de un argumento válido. ■

Reglas derivadas

A partir de estas reglas básicas y de toda la potencia del cálculo de primer orden, pueden demostrarse las siguientes propiedades.

Teorema 5.17 (Propiedades de equivalencia)

Reflexividad (ReflId): $t_0 = t_0$

Simetría (SimId): $$\frac{t_0 = t_1}{t_1 = t_0}$$

Transitividad (TransId): $$\frac{t_0 = t_1 \quad t_1 = t_2}{t_0 = t_2}$$

Observación 5.6.0.— Pudiésemos haber formulado estas reglas derivadas como teoremas lógicos:

Reflexividad (ReflId): $\vdash (\forall x)(x = x)$

Simetría (SimId): $\vdash (\forall x)(\forall y)(x = y \to y = x)$

Transitividad (TransId): $\vdash (\forall x)(\forall y)(\forall z)(x = y \land y = z \to x = z)$

Observación 5.6.1.— Notemos que $=$ es una relación de equivalencia y recordémoslo cuando las estudiemos[13].

Teorema 5.18 (Propiedad de intercambio (IntId))

$$\frac{t_0 = t_1}{Pt_0 \leftrightarrow Pt_1}$$

Observación 5.6.2.— Igualmente, pudiésemos haber formulado IntId como teorema:

$$\vdash (\forall x)(\forall y)(x = y \to (Px \leftrightarrow Py))$$

[13] *Cfr. infra* § 11.22 (pág. 628 de esta edición).

Observación 5.6.3.— La propiedad de intercambio (IntId) es justamente el *principio de indiscernibilidad de los idénticos*[14].

§ 5.6.1 Lógica y cálculo de primer orden con descripciones

A veces utilizamos circunloquios para no repetir nombres en el discurso o, a veces, cuando no recordamos un nombre o lo ignoramos. Por ejemplo, decimos «quien escribió Claros del bosque» o si recordamos que fue una mujer, «la autora de Claros del bosque». En ambos casos nos referimos, indirectamente, mediante una descripción, a María ZAMBRANO.

Para poder trabajar con descripciones, añadimos al lenguaje de la lógica de primer orden con identidad, $\mathcal{L}_1^=$, el signo ι que llamaremos *descriptor definido* o, simplemente, *descriptor*.

Descripciones definidas

Una *descripción definida* presupone la existencia y unicidad de la entidad a la que se refiere.

Para su formalización, introducimos el *descriptor definido* —que también llamamos, simplemente, *descriptor* y, a veces, *operador iota*— designado por ι.

Cuando se dan ambas condiciones, de existencia y unicidad de la entidad, decimos que se trata de una *descripción definida propia* (DDP); en caso contrario, hablamos de *descripción definida impropia* (DDI).

Ejemplo 208

Formalicemos la expresión «la obra más conocida de Miguel de Cervantes» en lógica de primer orden con descripciones.

Resolución.— Sea $Mxy \leftrightharpoons x$ es la obra más conocida de y y $c \leftrightharpoons$ Miguel de Cervantes, entonces $\iota xMxc$ representa la expresión anterior. En este caso se trata de una descripción definida propia. ■

Ejemplo 209

Formalicemos en lógica de primer orden con descripciones:

0. quien atracó el banco CUC;
1. el robot que atracó el banco CUC.

Resolución.—

[14] *Cfr. supra* § 5.1 (pág. 406 de esta edición).

0. si $Axy \leftrightharpoons x$ atracó el banco y, y $b \leftrightharpoons$ CUC, entonces la formalización de la descripción es

$$\iota x A x b.$$

1. si $Rx \leftrightharpoons x$ es un robot, $Axy \leftrightharpoons x$ atracó el banco y, y $b \leftrightharpoons$ CUC, entonces la descripción queda formalizada por

$$\iota x(Rx \wedge Axb).$$ 

Es posible expresar esta doble condición, de existencia y unicidad, definiendo un nuevo cuantor.

Definición 5.6.— El *singularizador*, también llamado *cuantor de existencia única*, que notamos $\exists!$ es, en realidad, una abreviatura:

$$\exists! x Px \leftrightharpoons \exists x(Px \wedge \forall y(Py \rightarrow x = y)).$$

Es posible caracterizar las descripciones definidas propias utilizando el singularizador:

$\iota x Ax$ es una descripción definida propia si, y sólo si, $\exists! x Ax$.

Observación 5.6.4.— Recordemos que hemos aludido a este cuantor anteriormente[15].

Observación 5.6.5.— Que sea posible formalizar una descripción, no asegura la existencia de la entidad descrita. Por ejemplo, si $Px \leftrightharpoons x$ es un número primo, y $Mxy \leftrightharpoons x$ es mayor que y, entonces es posible formalizar la descripción

el mayor de todos los (números) primos,

como

$$\iota x(Px \wedge \forall y(Py \rightarrow Mxy)).$$

Sin embargo, tal número no existe[16].

Reglas básicas

Aunque en su cálculo de descripciones Kalish y Montague también proporcionan una regla básica para las descripciones definidas impropias, nosotros adoptaremos sólo una regla básica.

Regla de descripción propia (D)

$$\frac{(\exists y)(\forall x)(Px \leftrightarrow x = y)}{P \iota x Px}$$

[15] *Cfr. v. gr. supra* § 4.1.3 (pág. 376).
[16] *Cfr. infra* teorema 18.16 (pág. 957).

Ejemplo 210

Siendo:

$$a \coloneqq \text{Claros del bosque},$$
$$Pxa \coloneqq x \text{ escribió } a,$$

entonces si es posible asegurar que la condición de ser quien escribió Claros del bosque únicamente es satisfecha por una persona, deduzcamos que quien escribió Claros del bosque escribió Claros del bosque.

Resolución.— En efecto, si es posible asegurar que la condición de ser quien escribió Claros del bosque únicamente es satisfecha por una persona, esto es, si

$$\exists y \forall x (Pxa \leftrightarrow x = y),$$

entonces la regla de descripción propia (D) nos permite introducir una descripción en el cálculo lógico incluso antes de recordar que se trata de María Zambrano; en efecto, siendo

$$\iota x Pxa \coloneqq \text{quien escribió Claros del bosque},$$

así, $\iota x Px$ es un término singular que es admisible introducir como sujeto y afirmar (es justo la consecuencia de la regla):

$$P(\iota x Pxa)a \coloneqq \text{quien escribió Claros del bosque escribió Claros del bosque.}$$ ■

Reglas derivadas

Teorema 5.19

(D*): $$\frac{(\forall x)(Px \leftrightarrow x = c)}{(\iota x)(Px = c)}$$

(D_o): $$\frac{(\forall x)(Px \leftrightarrow x = \iota x Px)}{(\exists y)(\forall x)(Px \leftrightarrow x = y)}$$ (doble línea)

Teorema 5.20

(D_1):
$$\begin{array}{l}(\exists y)(\forall x)(Px \leftrightarrow x = y)\\ Pc\\ \hline c = \iota x Px\end{array}$$

(D_2):
$$\begin{array}{l}(\exists y)(\forall x)(Px \leftrightarrow x = c)\\ c = \iota x Px\\ \hline Pc\end{array}$$

Actividad 5.2

Expresemos la regla: si queremos referirnos a la entidad x y ésta es una entidad indefinida y singular, entonces ha de anteponerse «una» a x.

Con miras a su resolución.— Una expresión lógico-matemática de esta regla es:

$$\begin{array}{l}\text{referir}(x)\\ \text{definida}(x)\\ \text{singular}(x)\\ \hline \text{anteponer}(x, \text{una})\end{array}$$

§ 5.6.2 Extensión aritmética de $\mathcal{L}_1$

Formalmente, para conseguir un poder expresivo adecuado para definir y relacionar la aritmética y la computabilidad, se añaden a $\mathcal{L}_1$, además del signo de igualdad, $=$ (constante predicativa), los signos correspondientes a las funciones adición y multiplicación, $+$ y $\cdot$ (constantes funtoriales), y los nombres propios de los números 0, 1, 2, . . .;[17] el nuevo lenguaje lo designamos por $\mathcal{L}_1^+$.

Ejemplo 211

En el conjunto de los números enteros positivos $\mathbb{Z}^+$, interpretemos las expresiones:

0. $\exists x \forall y \exists z(y + z = x)$;
1. $\exists z(y \cdot z = x)$;
2. $\neg(x = 1) \wedge \forall y(y | x \rightarrow (y = 1 \vee y = x))$.

Resolución.—

0. la expresión $\exists x \forall y \exists z(y + z = x)$ se interpreta como la existencia de un número natural x mayor que todos los demás;

[17] Esto de añadir una infinitud de nombres propios —en definitiva, el conjunto $\mathbb{N}$ de números naturales—, cosa que puede inquietarnos en este momento, lo resolveremos en § 15.0.2 (pág. 788 de esta edición), tras aprender a construir $\mathbb{N}$, pues bastará añadir el nombre propio del número cero, 0, y un funtor monádico denotativo de la operación «sucesor de».

1. la expresión $\exists z(y \cdot z = x)$ se interpreta como la definición de la relación diádica de divisibilidad $y \mid x$;

2. la expresión $\neg(x = 1) \wedge \forall y(y \mid x \rightarrow (y = 1 \vee y = x))$ se interpreta como la definición de ser x un número primo. ■

En $\mathcal{L}_1^+$, adicionalmente, resulta de interés operativo considerar el *recuento cuantificado* N que Dijkstra define y nota en la forma

$$(\text{cuantor variable} : \text{rango de la variable} : \text{predicado o función en la variable})\,.$$

Así, explicitado el rango de una variable como un intervalo natural, una definición recursiva en $\mathbb{N}$ es:

$$\begin{cases} (\mathrm{N}\, x : 0 \leq x < 0 : Px) = 0, \\ (\mathrm{N}\, x : 0 \leq x < n+1 : Px) = \begin{cases} (\mathrm{N}\, x : 0 \leq x < n : Px) + 1 & \text{si } Px, \\ (\mathrm{N}\, x : 0 \leq x < n : Px) & \text{si } \neg Px. \end{cases} \end{cases}$$

Observemos que dada una variable x con rango $r(x)$ y un predicado Px, $(\mathrm{N}\, x : r(x) : Px)$ es el número de valores distintos x en el rango $r(x)$ que satisfacen Px.

Ejemplo 212

Hallemos el recuento cuantificado N para un predicado en $\mathbb{N}$, digamos $Px \leftrightharpoons$ x es par, y el rango de x es $0 \leq x < n$.

Resolución.— En $\mathbb{N}$, para $Px \leftrightharpoons$ x es par y el rango de x es $0 \leq x < n$, entonces

$$(\mathrm{N}\, x : r(x) : Px) = \begin{cases} \frac{n}{2} + 1 & \text{si } n \text{ es par,} \\ \frac{n-1}{2} + 1 & \text{en caso contrario.} \end{cases}$$ ■

Es posible definir los cuatro cuantores estudiados de la lógica de primer orden, el generalizador, el particularizador, el singularizador y la función cuantorial de existencia no global, en función del recuento cuantificado N. En efecto, escribiendo A y E por $\forall$ y $\exists$, como propone Dijkstra, tenemos:

$$\begin{aligned} (\mathrm{A}\, x : 0 \leq x < n : Px) &= ((\mathrm{N}\, x : 0 \leq x < n : \neg Px) = 0); \\ (\mathrm{E}\, x : 0 \leq x < n : Px) &= ((\mathrm{N}\, x : 0 \leq x < n : Px) \geq 1); \\ (\mathrm{E!}\, x : 0 \leq x < n : Px) &= ((\mathrm{N}\, x : 0 \leq x < n : Px) = 1); \\ (\mathrm{E}^\circ\, x : 0 \leq x < n : Px) &= (1 \leq (\mathrm{N}\, x : 0 \leq x < n : Px) < n). \end{aligned}$$

Por motivos de brevedad y generalidad, es admisible omitir escribir el rango aunque asumimos que cuando lo hacemos en una igualdad se trata del mismo en ambos miembros, por ejemplo, las

leyes de De Morgan:

$$\neg(\mathrm{E}\,x :: Px) = (\mathrm{A}\,x :: \neg Px),$$
$$(\neg(\mathrm{N}\,x :: Px) \geq 1) = ((\mathrm{N}\,x :: Px) = 0),$$

y

$$\neg(\mathrm{A}\,x :: Px) = (\mathrm{E}\,x :: \neg Px),$$
$$(\neg(\mathrm{N}\,x :: \neg Px) = 0) = ((\mathrm{N}\,x :: \neg Px) \geq 1).$$

Por otro lado, análogamente, si f es una función de dominio $\mathbb{N}$, podremos usar los cuantores aritméticos suma y producto y denotar por $(\Sigma\, x : 0 \leq x < X : f(x))$ la suma de $f(x)$ recorriendo x el rango $0 \leq x < X$ y por $(\Pi\, x : 0 \leq x < X : f(x))$ el producto de $f(x)$ recorriendo x el rango $0 \leq x < X$. Observemos que podremos usar cualquier otro conjunto numérico en vez de $\mathbb{N}$ y cualquier otro rango.

Observación 5.6.6.— Dijkstra propone inicialmente la notación $\langle x : Rx : Px\rangle$ —con x la variable muda, Rx el rango de x y Px la descripción de los elementos del conjunto en términos de x— como alternativa mejorada a la notación $\{Px : Rx\}$ estándar (ISO 80000-2:2019) para conjuntos. Él proporciona el siguiente ejemplo:

$$\{i^n : i < n\}$$

preguntándose si este conjunto corresponde a $\{0^n, 1^n, 2^n, \ldots, (n-1)^n\}$ o a $\{i^{i+1}, i^{i+2}, i^{i+3}, \ldots\}$. La notación que él propone permite deshacer la ambigüedad y elegir entre:

$$\langle i : i < n : i^n\rangle = \{0^n, 1^n, 2^n, \ldots, (n-1)^n\},$$
$$\langle n : i < n : i^n\rangle = \{i^{i+1}, i^{i+2}, i^{i+3}, \ldots\}.$$

Asimismo, Dijkstra declara que no tiene ninguna objeción para incluir el tipo de la variable en la expresión, por ejemplo,

$$\langle i \in \mathbb{N} : i < n : i^n\rangle$$

aunque prefiere y siempre lo hará en el contexto que rodea a la expresión y nunca como parte de ella.

Cuando propuso esta notación en 1980[18] lo hizo con paréntesis, pero en 2000[19] declara que «la transición a paréntesis angulares fue una gran mejora».

Por nuestra parte, para conjuntos seguiremos usando la notación estándar (ISO 80000-2:2019) y nos la compondremos para despejar la ambigüedad, explicitando convenientemente el rango para que implícitamente indique cuál es la variable, por ejemplo,

$$\{i^n : n \in \mathbb{N} \wedge i < n\},$$

[18] https://www.cs.utexas.edu/users/EWD/transcriptions/EWD07xx/EWD737.html.
[19] https://www.cs.utexas.edu/users/EWD/transcriptions/EWD13xx/EWD1300.html.

y si no es suficiente, mediante el propio nombre del conjunto:

$$X_i = \{i^n : n \in \mathbb{N} \wedge i < n\},$$

y si aún queda lugar a dudas, recurriendo a la definición por extensión del conjunto:

$$\begin{aligned} X_i &= \{i^n : n \in \mathbb{N} \wedge i < n\} \\ &= \{i^{i+1}, i^{i+2}, i^{i+3}, \ldots\}. \end{aligned}$$

Actividad 5.3

¿A qué conjunto corresponde éste en notación de DIJKSTRA, $\langle i, n : i < n : i^n \rangle$?

§ 5.7 Inferir no es sólo deducir

Si bien usamos el pensamiento deductivo en el día a día, a menudo cometemos errores. Cuatro razones podrían ser —*cfr.* BENNET [105] (pág. 24)—:

0.ª, ignoramos información disponible;

1.ª, añadimos información por nuestra cuenta (y riesgo);

2.ª, tenemos problemas a la hora de hacer un seguimiento de la información, y

3.ª, no somos capaces de recuperar información necesaria.

Como sigue exponiendo la profesora BENNETT, por una parte, mientras que algunas investigaciones sugieren que sea debido a las diferentes naturalezas de las lenguas naturales frente a los lenguajes formales, otras apuntan a que sea debido a una cierta inhabilidad cognitiva, y, por otra parte, mientras que algunas investigaciones indican que cierto grado de familiaridad con el tema de un argumento potencia nuestra habilidad para inferir correctamente, otras destacan que sea precisamente esa familiaridad la que interfiere con nuestra pericia.

En cualquier caso, no es la deducción la única vía de inferencia. En efecto, a continuación identificamos como vías de inferencia, además de la deducción, la aducción, sea inducción o educción, la abducción, la transducción y la retroducción.

§ 5.7.0 Aducción, sea ésta inducción o educción

La *aducción* comprende la inducción y la educción.

Definición 5.7.— La *inducción* va desde la muestra a la población. En concreto, de saber que estamos ante una muestra ϕ_j que procede de una población determinada j y de observar en la muestra el hecho ψ de que una propiedad es satisfecha por todas las unidades de la muestra, inferir la conclusión χ_j

de que dicha propiedad la satisfacen todas las unidades de dicha población; esquemáticamente,

$$\{\phi_j, \psi\} \vdash \chi_j.$$

Ejemplo 213

Sean:
$\phi_j \fallingdotseq$ Estas magdalenas las hemos extraído de esta bolsa. (Muestra de la población j)
$\psi \fallingdotseq$ Estas magdalenas tienen sabor a limón. (Hecho observable en la muestra)
$\chi_j \fallingdotseq$ Las magdalenas de esta bolsa tienen sabor a limón. (Población j)
$\tau_j \fallingdotseq$ La siguiente magdalena que extraigamos de esta bolsa j tiene sabor a limón. (Subpoblación de j)
En esta interpretación, proporcionemos un ejemplo de inducción.

Resolución.— Un ejemplo de inducción es el siguiente: como estas magdalenas las hemos extraído de esta bolsa (ϕ_j) y todas (las extraídas) tienen sabor a limón (ψ), entonces (inducimos) que todas las magdalenas de esta bolsa tienen sabor a limón (χ_j). ∎

Definición 5.8.— La *educción* va desde la muestra a la subpoblación. Concretamente, de saber que estamos ante una muestra ϕ_j que procede de una población determinada j y de observar en la muestra el hecho ψ de que una propiedad es satisfecha por todas las unidades de la muestra, inferir que dicha propiedad la satisfará una subpoblación τ_j cualquiera de la población j; esquemáticamente,

$$\{\phi_j, \psi\} \vdash \tau_j.$$

Ejemplo 214

Dada la interpretación del ejemplo 213 (433 de esta edición), proporcionemos un ejemplo de educción.

Resolución.— Un ejemplo de educción es el siguiente: como estas magdalenas las hemos extraído de esta bolsa (ϕ_j) y todas (las extraídas) tienen sabor a limón (ψ), entonces (educimos) que la siguiente magdalena que extraigamos de esta bolsa tendrá sabor a limón (τ_j). ∎

§ 5.7.1 Deducción y abducción

Tanto la deducción como la abducción van desde la población a la muestra.

Definición 5.9.— En la *deducción*, de saber el hecho χ_j de que una propiedad se satisface en toda una población j y de saber que estamos ante una muestra ϕ_j que procede de dicha población j, inferir la conclusión ψ de que dicha propiedad se satisface en dicha muestra; esquemáticamente,

$$\{\chi_j, \phi_j\} \vdash \psi.$$

Ejemplo 215

Dada la interpretación del ejemplo 213 (433 de esta edición), proporcionemos un ejemplo de deducción.

Resolución.— Un ejemplo de deducción es el siguiente: como todas las magdalenas de esta bolsa tienen sabor a limón (χ_j) y estas magdalenas las hemos extraído de esta bolsa (ϕ_j), entonces (deducimos) que todas estas magdalenas (las extraídas) tienen sabor a limón (ψ). ■

Definición 5.10.— En la *abducción*, de saber el hecho χ_j de que una propiedad se satisface en toda una población j y de observar en la muestra el hecho ψ de que dicha propiedad es satisfecha por todas las unidades de la muestra, inferir la conclusión (ϕ_j) de que dicha muestra procede de dicha población j; esquemáticamente,

$$\{\chi_j, \psi\} \vdash \phi_j.$$

Ejemplo 216

Dada la interpretación del ejemplo 213 (433 de esta edición), proporcionemos un ejemplo de abducción.

Resolución.— Un ejemplo de abducción es el siguiente: como todas las magdalenas de esta bolsa tienen sabor a limón (χ_j) y estas magdalenas (las extraídas) tienen sabor a limón (ψ), entonces (abducimos) que estas magdalenas las hemos extraído de esta bolsa (ϕ_j). ■

§ 5.7.2 Transducción

Tras el estudio y la práctica se generan esquemas mentales a los que acudimos como posibles modelizaciones de situaciones nuevas, es decir, expresamos un problema nuevo con el vocabulario de problemas antiguos ya resueltos. Esto hacemos, por ejemplo, con los *modelos de urnas y bolas* en *teoría de la probabilidad*.

Definición 5.11.— La *transducción* transforma la situación original en una «imaginaria» por analogía; esquemáticamente,

$$X \leftarrow \phi_j,\ Y \leftarrow \psi,\ Z \leftarrow \chi_j.$$

Observación 5.7.0.— Insistamos, la transducción no es más que un proceso optativo de abstracción transversal, fundamentado en el conocimiento o experiencia que valide la analogía y previo a cualquiera de las otras vías de inferencia.

Ejemplo 217

Dada la interpretación del ejemplo 213 (433 de esta edición), proporcionemos un ejemplo de transducción.

Resolución.— Un ejemplo de transducción es el siguiente. Sean:

$X \risingdotseq$ Estas bolas las hemos extraído de esta urna. (Muestra)

$Y \risingdotseq$ Estas bolas son rojas. (Hecho observable en la muestra)

$Z \risingdotseq$ Las bolas de esta urna son rojas. (Población j)

Esto es, elegimos el modelo de bolas (de color rojo) y urnas para representar la cuestión: una bola designa una magdalena, una bola roja, una magdalena con sabor a limón y una urna, una bolsa. Así,

$\tau_j \risingdotseq$ La siguiente bola que extraigamos de esta urna j es roja. (Subpoblación de j)

Otro ejemplo pudiese ser:

$\phi_j \risingdotseq$ Estas personas han venido por este camino. (Muestra)

$\psi \risingdotseq$ Estas personas hablan español. (Hecho observable en la muestra)

$\chi_j \risingdotseq$ Todas las personas que vengan por ese camino hablan español. (Población j)

$\tau_j \risingdotseq$ La próxima persona que venga por el camino j habla español. (Subpoblación de j) ■

Entonces, asumiendo que una bola designe a una persona, una urna un camino y que el hecho de ser roja designe al hecho de hablar español, pudiésemos transducir similarmente a lo anterior.

§ 5.7.3 Retroducción

Definición 5.12.— En la *retroducción*[20], vamos desde la muestra a la población. En concreto, de saber que estamos ante una reunión $\bigwedge_j \phi_j$ de muestras —una nueva muestra fabricada por abstracción transfigurativa— que proceden cada una ϕ_j de una población determinada j y observar que una pro-

[20] No la confundamos con la retroducción de Peirce, que es el modo AII de la II.ª figura del silogismo categórico.

piedad es satisfecha por todas las unidades de la reunión de muestras (ψ), inferir (por inducción) la conclusión $\bigwedge_j \chi_j$ de que dicha propiedad la satisfacen todas las unidades de la reunión de poblaciones; esquemáticamente,

$$\left\{\bigwedge_j \phi_j, \psi\right\} \vdash \bigwedge_j \chi_j.$$

Ejemplo 218

Se trata de elegir la «mejor» persona para un puesto de trabajo.

Resolución.— Pudiese hacerse en tres fases consecutivas: una inducción, una retroducción y una abducción. En efecto,

0.º *Inducción*: Para cada organización j se razona así: «[ϕ_j] "Esta persona de esta organización j es quien mejor desempeña ese puesto" *y* [ψ] "esta persona posee las características C_j", *luego* [χ_j] "la mejor persona de esta organización j para desempeñar ese puesto posee las características C_j"».

1.º *Retroducción:* «[$\bigwedge_j \phi_j$]"Estas personas son las mejores en el desempeño de ese puesto en sus organizaciones" *y* [ψ]"estas personas poseen las características $\gamma(C_1, \ldots, C_n)$", *luego* [$\bigwedge_j \chi_j$] "la mejor posee las características $\gamma(C_1, \ldots, C_n)$"» (γ indica una función o procedimiento de agregación, por ejemplo, una media aritmética, ponderada, etc. —$\gamma(C_1, \ldots, C_n)$ indica un conjunto de características resultado de dicha agregación de características procedentes de las distintas organizaciones—).

2.º *Abducción:* «[χ_i] "La mejor posee las características $\gamma(C_1, \ldots, C_n)$" (las personas de la población i de las mejores tiene esas características) *y* [ψ] "esta persona posee las características $\gamma(C_1, \ldots, C_n)$" (muestra de tamaño 1), *luego* [ϕ_i] "esta persona es la mejor" (esta persona la hemos "extraído" de la población i de las mejores)». ■

Sea la vía de inferencia que sea, deberíamos precavernos de las actitudes reduccionistas —incluso, a veces, populistas— que siempre nos acechan de imaginar y adoptar jerarquías basadas en considerandos personales acerca de la importancia estructural de las entidades participantes, haciendo, por ejemplo, que juzguemos a unas como aderezos o transformaciones de otras, cuando la realidad puede ser bien distinta.

Agentes software

Pudiese ser que en determinadas instancias nos represente un *agente software* (fuere en entornos de comercio electrónico con una oferta excesiva, o de apoyo si, por ejemplo, tenemos discapacidad visual, o en general, como sistemas de ayuda en la llamada Web Semántica y en las Web $m.n$ que surjan). Las arquitecturas de los agentes software admiten múltiples clasificaciones, según los criterios que se elijan. En particular, en cuanto a su interacción con el entorno, suele distinguirse entre reactivos, deliberativos e híbridos:

— Un *agente reactivo* atiende sólo al presente y actúa según un esquema estímulo-respuesta.

— Un *agente deliberativo* integra un modelo simbólico del entorno y logra conclusiones vía alguna lógica formal o gramática parda (a base de heurística y seudológica).

— Un *agente híbrido* combina características de los dos tipos anteriores.

Pudiésemos decir que tanto la acción de los agentes deliberativos como la de los híbridos muestra que ambos tienen la capacidad de hacer inferencias.

Claro que es posible refinar esta clasificación considerando atributos más específicos[*]: *agentes autónomos*, proactivos, dirigidos por objetivos o metas; *agentes colaborativos*, comprometidos con dialogar y cooperar, *agentes adaptativos*, persistentes, con estados internos que se actualizan según la experiencia, y *agentes móviles*. Si nos inquietase conocer más sobre ellos, pudiésemos tomar como punto de partida, por ejemplo, el libro *Intelligent Software Agents*, de Brenner, Zarnekov y Wittig [106].

Por otra parte, puede que determinados agentes software nos ayuden en nuestras tareas; un ejemplo es el *sistema multiagente AI co-scientist*, de Google, donde seis agentes especializados —de nombres, Generación, Reflexión, Clasificación, Evolución, Proximidad y Meta-revisión—, además de un agente supervisor (aparentemente, todo un verdadero *equipo de agentes software*), hacen que el sistema tenga ciertas funcionalidades de colaborador científico en línea[†].

[*] Según Oren Etzioni y Daniel S. Weld, Intelligent Agents on the Internet: Fact, Fiction and Forecast, *IEEE Expert* 10(4):44–49, 1995.

[†] https://research.google/blog/accelerating-scientific-breakthroughs-with-an-ai-co-scientist/.

§ 5.8 Bibliografía

- Para una primera aproximación:

[62] María Manzano Arjona y Antonia Huertas Sánchez. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

[99] Amador ANTÓN ANTÓN y Pascual CASAÑ MUÑOZ. *Lógica matemática. II. Lógica de predicados*. NAU llibres, Valencia, España, 1998.

- Para estudiar, practicar y conocer más:

[64] Manuel GARRIDO GIMÉNEZ. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

[65] Carmen GARCÍA TREVIJANO. *El arte de la lógica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1999.

- Para profundizar, acullá:

[66] Manuel GARRIDO GIMÉNEZ, Luis Manuel VALDÉS VILLANUEVA, Jesús MOSTERÍN DE LAS HERAS, Alfonso GARCÍA SUÁREZ y Carlos-Peregrín FERNÁNDEZ OTERO. *Lógica y lenguaje*. Cuadernos de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1989.

[67] Raymond Merrill SMULLYAN. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

[60] Herbert Bruce ENDERTON. *A mathematical introduction to logic*. Harcourt/Academic Press, San Diego, Condado de San Diego, California (US-CA), Estados Unidos de América, 2.ª ed., 2001.

Capítulo 6

De la metalógica

¿Me contradigo? Muy bien, entonces me contradigo, (soy grande, contengo multitudes).
(Walt Whitmann (1819-1892), *Song of Myself*).

¿Existe alguna relación entre lo válido y lo deducible, entre lo verdadero y lo derivable formalmente? Además de la corrección y la completitud que responderán a esta inquietud, son tres más las cuestiones metalógicas sobre un sistema formal que nos preocupan y que estudiaremos en este capítulo, cinco en total:

0. *Corrección*: debe suceder en el sistema que todo lo deducible sintácticamente sea también deducible semánticamente.
1. *Consistencia*: el sistema no debe contener ninguna fórmula que sea teorema lógico y cuya negación sea también teorema lógico.
2. *Completitud*: debe suceder en el sistema que todo lo deducible semánticamente sea también deducible sintácticamente.
3. *Compacidad*: la satisfactibilidad de un conjunto infinito numerable de fórmulas del sistema debe ser consecuencia de la satisfactibilidad de todos los subconjuntos finitos de dicho conjunto.
4. *Decidibilidad*: debe existir un procedimiento que permita conocer si una fórmula dada es deducible en el sistema.

§ 6.0 Metalógica de la lógica de juntores

La metalógica es el estudio de la metateoría de la lógica, esto es, el objeto de estudio en la metalógica es la propia lógica, por ejemplo, sus propiedades.

Uno de los fines implícitos en el desarrollo de cualquier teoría formal es que su teoría de modelos y su teoría de la demostración coincidan en su expresividad, en el sentido de que lo que sea deducible semánticamente lo sea también sintácticamente, y viceversa.

§ 6.0.0 Corrección y consistencia

Veamos que

- *la lógica de juntores es correcta*, esto es, que en ella todo lo deducible sintácticamente también lo es semánticamente, y que
- *la lógica de juntores es consistente*, es decir, que está exenta de contradicciones.

Definición 6.0.— Un *sistema deductivo consistente* es aquél en el que no existe ninguna fórmula ϕ tal que $\vdash \phi$ y $\vdash \neg\phi$, simultáneamente. En caso contrario, decimos que es *inconsistente*.

Definición 6.1.— Sea Φ un conjunto de fórmulas. Si existe una fórmula ϕ tal que $\Phi \vdash \phi$ y $\Phi \vdash \neg\phi$, decimos que Φ es *conjunto inconsistente de fórmulas*. Caso contrario, se dice *consistente*.

Ejemplo 219

Demostremos que el conjunto $\{p \to q, \neg q, p\}$ es un conjunto inconsistente de fórmulas.

Resolución.— En efecto. Veamos primero que $\{p \to q, \neg q, p\} \vdash p$. La derivación formal que lo consigue es bien sencilla:

0. p DF1

Por otro lado, en el ejemplo 2.0.3 (pág. 183 de esta edición), vimos que $\{p \to q, \neg q\} \vdash \neg p$. Como $\{p \to q, \neg q\}$ es un subconjunto de $\{p \to q, \neg q, p\}$, entonces por la propiedad de monotonía —*vid. supra* teorema 2.2 (pág. 188 de esta edición)—, se tiene que $\{p \to q, \neg q, p\} \vdash \neg p$.

Por lo tanto, $\{p \to q, \neg q, p\}$ es un conjunto inconsistente de fórmulas. ■

Observación 6.0.0.— Pudiésemos utilizarla celda libre de computación de SageMath° para saber de la consistencia de dicho conjunto:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
# referencia: https://doc.sagemath.org/html/en/reference/logic/index.html
f, g, h = propcalc.get_formulas("p->q", "~q", "p") # introducimos el conjunto de fórmulas
propcalc.consistent(f, g, h) # mostramos si es un conjunto consistente
```

Teorema 6.0
Si Φ es un conjunto inconsistente de fórmulas, entonces $\Phi \vdash \phi$, sea cual sea la fórmula ϕ.

Como lo que afirma el teorema anterior es para toda fórmula, un corolario importante suyo es que de un conjunto inconsistente de fórmulas pudiese deducirse formalmente una fórmula insatisfactible; en otras palabras, a partir de la inconsistencia pudiese deducirse la verdad de lo falso.

Actividad 6.0
Demostremos que $\{p \to q, \neg q, p\} \vdash q \wedge \neg q$.

Teorema 6.1 (Reducción al absurdo (abreviadamente Abs, también RAA))
Sean ϕ una fórmula y Φ un conjunto de fórmulas, entonces $\Phi \cup \{\neg\phi\}$ es un conjunto inconsistente de fórmulas si, y sólo si, $\Phi \vdash \phi$.

Ejemplo 220

Demostremos que q se deriva inmediatamente de $\{p \to q, p\}$

Resolución.— Sea $\Phi = \{p \to q, p\}$ y sea ϕ la fórmula q. En el teorema 219 (pág. 441 de esta edición) demostramos que $\Phi \cup \{\neg q\}$ es un conjunto inconsistente de fórmulas, por lo que, por el teorema anterior (RAA), q se deriva inmediatamente de Φ. ■

Observación 6.0.1.— Lo que demuestra este ejemplo quedaba ya recogido en el silogismo hipotético en su forma *modus ponendo ponens*: $\{p \to q, p\} \vdash q$.

Definición 6.2.— Una teoría formal satisface la *propiedad de corrección, rectitud o validez* (decimos que dicha teoría formal es *correcta*), precisamente si para todo conjunto Φ de fórmulas y para toda fórmula ϕ, sucede que

$$\text{si } \Phi \vdash \phi \text{, entonces } \Phi \vDash \phi,$$

° *Vid.* https://sagecell.sagemath.org/.

—esto es, que la derivabilidad sintáctica asegura la derivabilidad semántica—. En particular, todo teorema lógico es una fórmula válida, es decir, se satisface que

$$\text{si } \vdash \phi \text{, entonces } \models \phi.$$

Observación 6.0.2.— Que se satisfaga la propiedad de corrección es extremadamente importante, pues simplifica enormemente la demostración. Pensemos que para asegurar que $\Phi \models \phi$ deberíamos corroborar que todas las interpretaciones son modelos, mientras que para asegurar que $\Phi \vdash \phi$ es suficiente con encontrar una deducción formal desde Φ a ϕ.

Observación 6.0.3.— Conseguir una teoría correcta no es difícil. Basta tomar como axiomas fórmulas válidas e imponer para las reglas de inferencia que conserven la validez, es decir, que la aplicación de una regla de inferencia sobre una fórmula válida produzca una fórmula válida.

Teorema 6.2 (Enunciado alternativo de la propiedad de corrección)
Un enunciado equivalente de la propiedad de corrección es:

Si un conjunto Φ de fórmulas es inconsistente, entonces Φ es insatisfactible.

Demostración.— En la propiedad de corrección,

$$\text{si } \Phi \vdash \phi \text{, entonces } \Phi \models \phi,$$

sustituyendo $\Phi \vdash \phi$ por su equivalente según el teorema 6.1 (pág. 442 de esta edición) se tiene que

$$\text{si } \Phi \cup \{\neg\phi\} \text{ es un conjunto inconsistente de fórmulas, entonces } \Phi \models \phi,$$

de donde, sustituyendo $\Phi \models \phi$ por su equivalente según el teorema 1.10 (pág. 147 de esta edición) se tiene que

si $\Phi \cup \{\neg\phi\}$ es un conjunto inconsistente de fórmulas,
entonces
$\Phi \cup \{\neg\phi\}$ es un conjunto insatisfactible de fórmulas,

y como en realidad $\Phi \cup \{\neg\phi\}$ es un conjunto arbitrario de fórmulas, se tiene que

todo conjunto inconsistente de fórmulas es un conjunto insatisfactible de fórmulas,

que abreviadamente escribimos, dado un conjunto Φ de fórmulas,

si Φ es inconsistente, entonces Φ es insatisfactible,

siendo todos y, en particular el último, enunciados equivalentes de la propiedad de corrección. ■

Teorema 6.3 (Teorema de rectitud (o de validez) (Post))
La lógica de juntores es correcta, esto es, para todo conjunto Φ de fórmulas y para toda fórmula ϕ, sucede que

$$\text{si } \Phi \vdash \phi, \text{ entonces } \Phi \vDash \phi.$$

Observación 6.0.4.— Por el teorema 6.2 (pág. 443 de esta edición), un enunciado equivalente del teorema de rectidud es: todo conjunto inconsistente de fórmulas es un conjunto insatisfactible de fórmulas.

Teorema 6.4 (Corolario del teorema de rectitud)
Si un conjunto de fórmulas es satisfactible, entonces es consistente.

En definitiva.

Teorema 6.5 (Consistencia de la lógica de juntores)
La lógica de juntores es consistente.

Demostración.— Caso contrario, si existiese una fórmula ϕ tal que $\vdash \phi$ y $\vdash \neg\phi$, simultáneamente, entonces, por el teorema de rectitud, $\vDash \phi$ y $\vDash \neg\phi$, simultáneamente, en contra de la definición de interpretación (ya que en ese caso existiría una fórmula ϕ tal que $I(\phi) = I(\neg\phi) = 1$, contrariamente a la redefinición de interpretación (*vid. supra* definición 1.17 [pág. 123 de esta edición]). ■

§ 6.0.1 Completitud

Veamos que *la lógica de juntores es completa*, esto es, que todo lo deducible semánticamente lo es también sintácticamente, en otras palabras, que el sistema formal, en particular, su sintaxis, es lo suficientemente expresiva y potente como para que con ella sean derivables todas las conclusiones que esperamos obtener.

Definición 6.3.— Una teoría formal satisface la *propiedad de completitud* —también decimos que dicha teoría formal es *completa*— precisamente si para todo conjunto Φ de fórmulas y para toda fórmula ϕ, sucede que

$$\text{si } \Phi \vDash \phi, \text{ entonces } \Phi \vdash \phi$$

—esto es, la derivabilidad semántica asegura la derivabilidad sintáctica—. En particular, toda fórmula válida es un teorema lógico, es decir, se satisface que

$$\text{si } \vDash \phi, \text{ entonces } \vdash \phi$$

Teorema 6.6 (Enunciado alternativo de la propiedad de completitud)
Un enunciado equivalente de la propiedad de completitud es:

Si un conjunto Φ de fórmulas es insatisfactible, entonces Φ es inconsistente.

Demostración.— En la propiedad de completitud,

$$\text{si } \Phi \vDash \phi \text{, entonces } \Phi \vdash \phi,$$

sustituyendo $\Phi \vdash \phi$ por su equivalente según el teorema 6.1 (pág. 442 de esta edición) se tiene:

$$\text{si } \Phi \vDash \phi \text{ entonces } \Phi \cup \{\neg\phi\} \text{ es un conjunto inconsistente de fórmulas,}$$

de donde, sustituyendo $\Phi \vDash \phi$ por su equivalente según el teorema 1.10 (pág. 147 de esta edición) se tiene:

si $\Phi \cup \{\neg\phi\}$ es un conjunto insatisfactible de fórmulas,
entonces
$\Phi \cup \{\neg\phi\}$ es un conjunto inconsistente de fórmulas,

y como en realidad $\Phi \cup \{\neg\phi\}$ es un conjunto arbitrario de fórmulas, se tiene que:

todo conjunto insatisfactible de fórmulas es un conjunto inconsistente de fórmulas,

que abreviadamente escribimos, dado un conjunto Φ de fórmulas:

si Φ es insatisfactible, entonces Φ es inconsistente,

siendo todos ellos y, en particular este último, enunciados equivalentes de la propiedad de completitud. ■

Teorema 6.7 (Reformulación de la propiedad de completitud)
Si un conjunto de fórmulas es consistente, entonces es satisfactible.

Así, el paso de la consistencia a la satisfactibilidad faculta el paso de la validez lógica a la derivabilidad.

Teorema 6.8 (Teorema de completitud (Post, 1920) (Kalmar, 1934-1935))
La lógica de juntores es completa, esto es, para todo conjunto Φ de fórmulas y para toda fórmula ϕ, de la lógica de juntores, sucede que

$$\text{si } \Phi \vDash \phi \text{, entonces } \Phi \vdash \phi,$$

y particularmente que

$$\text{si } \vDash \phi \text{, entonces } \vdash \phi.$$

Demostración.— Pudiésemos estudiarla, por ejemplo, en Garrido [64] (págs. 313–315). ■

Observación 6.0.5.— Por el teorema 6.6 (pág. 445 de esta edición), un enunciado equivalente del teorema de completitud es: todo conjunto insatisfactible de fórmulas es un conjunto inconsistente de fórmulas.

La conjunción del teorema de rectitud con el de completitud demuestra el siguiente corolario.

Teorema 6.9 (Corolario: la lógica de juntores es correcta y completa)
Para todo conjunto Φ de fórmulas y para toda fórmula ϕ,

$$\Phi \vDash \phi \text{ si, y sólo si, } \Phi \vdash \phi.$$

Observación 6.0.6.— Por lo visto anteriormente, un enunciado equivalente de este corolario es:

todo conjunto inconsistente de fórmulas es un conjunto insatisfactible de fórmulas y, recíprocamente, todo conjunto insatisfactible de fórmulas es un conjunto inconsistente de fórmulas,

o dicho más brevemente,

un conjunto de fórmulas es inconsistente si, y sólo si, es insatisfactible,

que, por lo discutido anteriormente, equivale a decir que

un conjunto de fórmulas es consistente si, y sólo si, es satisfactible.

Observación 6.0.7.— A modo de resumen, los teoremas anteriores suelen expresarse:

0.°, en términos de insatisfactibilidad e inconsistencia:

- (corrección): Φ es inconsistente sólo si Φ es insatisfactible;
- (completitud): Φ es inconsistente si Φ es insatisfactible;
- (corrección y completitud): Φ es inconsistente si, y sólo si, Φ es insatisfactible;

1.°, en términos de satisfactibilidad y consistencia:

- (corrección): Φ es satisfactible sólo si Φ es consistente;
- (completitud): Φ es satisfactible si Φ es consistente;
- (corrección y completitud): Φ es satisfactible si, y sólo si, Φ es consistente;

2.°, en términos de teoremas lógicos y fórmulas válidas:

- (corrección): $\vdash \phi$ sólo si $\vDash \phi$ (ϕ es un teorema lógico sólo si ϕ es una fórmula válida);
- (completitud): $\vdash \phi$ si $\vDash \phi$ (ϕ es un teorema lógico si ϕ es una fórmula válida);
- (corrección y completitud): $\vdash \phi$ si, y sólo si, $\vDash \phi$ (ϕ es un teorema lógico si, y sólo si, ϕ es una fórmula válida);

3.°, en términos conjuntistas:

- (corrección): $\{\phi : \Phi \vdash \phi\} \subseteq \{\phi : \Phi \vDash \phi\}$;
- (completitud): $\{\phi : \Phi \vdash \phi\} \supseteq \{\phi : \Phi \vDash \phi\}$;
- (corrección y completitud): $\{\phi : \Phi \vdash \phi\} = \{\phi : \Phi \vDash \phi\}$.

Observación 6.0.8.— Reescribamos:

- «toda la verdad» (completitud: todo teorema lógico —sintaxis— es una fórmula válida —semántica— [todo lo que es demostrable (derivable formalmente) es de hecho verdadero]);
- «nada más que la verdad» (corrección: toda fórmula válida es un teorema lógico —todo lo que es verdad tiene una demostración (una derivación formal)—);
- «toda la verdad y nada más que la verdad» (completitud y corrección: los teoremas lógicos son, y sólo son, las fórmulas válidas).

Ejemplo 221

Supongamos que ϕ y ψ son fórmulas lógicamente equivalentes. Sea χ una fórmula cualquiera. ¿Es $(\phi \to \chi) \leftrightarrow (\psi \to \chi)$ un teorema lógico?

Resolución.— Como la lógica de juntores es correcta y completa, la cuestión equivale a saber si $(\phi \to \chi) \leftrightarrow (\psi \to \chi)$ es una fórmula válida.

Como por hipótesis, ϕ y ψ son fórmulas lógicamente equivalentes, $\phi \leftrightarrow \psi$ es una fórmula válida, por lo que los valores de verdad de ϕ y ψ son iguales, y por tanto, la tabla de verdad queda

ϕ	ψ	χ	$(\phi$	$\to$	$\chi)$	$\boxed{\leftrightarrow}$	$(\psi$	$\to$	$\chi)$
1	1	1	1	1	1	1	1	1	1
1	1	0	1	0	0	1	1	0	0
0	0	1	0	1	1	1	0	1	1
0	0	0	0	1	0	1	0	1	0

es decir, se satisface que

$$\vDash (\phi \to \chi) \leftrightarrow (\psi \to \chi)$$

—esto es, $(\phi \to \chi) \leftrightarrow (\psi \to \chi)$ es una fórmula válida— y por tanto, por el teorema 6.8 de completitud de KALMAR (pág. 445 de esta edición), también se satisface que:

$$\vdash (\phi \to \chi) \leftrightarrow (\psi \to \chi)$$

—esto es, $(\phi \to \chi) \leftrightarrow (\psi \to \chi)$ es un teorema lógico. ∎

Observación 6.0.9.— Conseguir una teoría completa no siempre es posible. Pensemos que el objetivo sería la caracterización sintáctica de la validez —es decir, de nuestra comprensión (semánti-

ca) de parte del mundo real. Ahondado un poco, pudiésemos distinguir y discutir sobre al menos tres tipos de validez: *validez etiológica*, ateniente al origen del contenido semántico; *validez descriptiva*, correspondiente a las características descriptoras de las entidades y conceptos incluidas en dicho contenido; *validez predictiva*, ésta es, si puede predecirse la interacción del educto en su entorno sintáctico (lo cual presupone la *verificación* del proceso de traducción).

§ 6.0.2 Decidibilidad

Veamos que *la lógica de juntores es decidible*, o sea, que existe al menos un procedimiento que permite conocer si una fórmula dada es deducible.

Procedimientos de deducción vs. procedimientos de refutación

La lógica de juntores es *decidible*, en el sentido de que siempre existe un método —un procedimiento de decisión sólido, completo y que termine— que decide si una fórmula es o no válida.

Hasta este momento conocemos cinco métodos. Tal y como los hemos utilizado hasta ahora, y dentro del conjunto general de procedimientos de demostración (en ámbito semántico o sintáctico), estos cinco se clasifican como *procedimientos de deducción*, y son:

- tablas de verdad;
- reglas de sustitución;
- formas normales;
- principios de dualidad;
- derivación formal.

Mas puede ocurrir que no seamos capaces de decidir con estos métodos o con esta forma de utilizarlos.

La otra gran colección de sistemas de demostración son los *procedimientos de refutación*.

Las tablas de verdad, las formas normales y las derivaciones formales pueden utilizarse como métodos de refutación, participando en las aplicaciones de los dos últimos las reglas de sustitución y los principios de dualidad.

Otros procedimientos de refutación son las *tablas analíticas*, ya estudiadas, y *resolución* (Robinson [107]).

Así que desde el punto de vista de la refutación, tenemos también cinco posibilidades, que son:

- tablas de verdad;
- formas normales;

- derivación formal;
- tablas analíticas/semánticas;
- resolución.

En un procedimiento de refutación, la idea que subyace es demostrar la validez de una fórmula (resp., inferencia deductiva) refutando la negación de dicha fórmula (resp., inferencia deductiva[1]). Esto se basa en las relaciones ya vistas siguientes. Siendo Φ un conjunto de fórmulas y ϕ una fórmula:

$$\begin{aligned}
\Phi \vDash \phi &\Leftrightarrow \Phi \cup \{\neg\phi\} \text{ es insatisfactible}\\
\phi \text{ es válida } &\Leftrightarrow \neg\phi \text{ es insatisfactible}\\
\Phi \vdash \phi &\Leftrightarrow \Phi \cup \{\neg\phi\} \text{ es inconsistente}\\
\phi \text{ es un teorema lógico } &\Leftrightarrow \neg\phi \text{ es inconsistente}
\end{aligned}$$

Ejemplo 222 Reducción al absurdo (Abs, RAA) / Demostración por contradicción

Imaginemos que queremos demostrar $\vdash \phi \to \psi$.

Resolución.— Que $\phi \to \psi$ sea un teorema lógico es equivalente a que $\neg(\phi \to \psi)$ sea inconsistente. Esto último pudiésemos demostrarlo, por ejemplo, viendo que $\neg(\phi \to \psi) \to \bot$, o su fórmula equivalente $(\phi \wedge \neg\psi) \to \bot$.

Como ya hemos dicho, este procedimiento es conocido clásicamente como *reducción al absurdo* (Abs, RAA) (o, sinónimamente, *demostración por contradicción*); en lógica de juntores, dada la afirmación «si ϕ, entonces ψ», si de suponer que se satisfacen simultáneamente su premisa ϕ y la negación de su conclusión $\neg\psi$, se deduce un absurdo (contradicción), esto significa que dicha afirmación es cierta, en otras palabras, que dicha afirmación es un teorema del sistema formal en el que se esté trabajando.

Notemos también que caso de que $\vdash \neg((\phi \wedge \neg\psi) \to \bot)$, como $\phi \to \psi \vdash (\phi \wedge \neg\psi) \to \bot$, se tendría $\vdash \neg(\phi \to \psi)$. ■

[1] Siendo Φ un conjunto de fórmulas y ϕ una fórmula, la negación de la inferencia deductiva $\Phi \vdash \phi$ es $\Phi \cup \{\neg\phi\}$.

Ejemplo 223

Si el hecho de que un gobierno tome unas medidas económicas arbitrarias y a la vez debilite los pilares fundamentales de la sociedad implica contradicciones sociales (por ejemplo, que dicho gobierno, elegido por los ciudadanos, no considere las demandas de los ciudadanos durante su legislatura), se deduce que caso de que un gobierno aplique unas medidas económicas arbitrarias debe reforzar los pilares fundamentales de la sociedad.

[SEL 3:5].

Resolución.— Sean $p \leftrightharpoons$ «un gobierno toma medidas económicas arbitrarias» y $q \leftrightharpoons$ «se refuerzan los pilares fundamentales de la sociedad».

Así que pudiésemos preguntarnos por la validez de la siguiente inferencia deductiva: $\{(p \wedge \neg q) \rightarrow \bot\} \vdash p \rightarrow q$. Llamémosla $\mathcal{A}$.

Veamos si $\mathcal{A}$ es válida. Razonemos vía su contraparte semántica, $\{(p \wedge \neg q) \rightarrow \bot\} \vDash p \rightarrow q$, con su forma lógica, a partir de suponer que ésta es falsa:

$(p$	$\wedge$	$\neg$	q	$\rightarrow_0$	$\bot)$	$\rightarrow_1$	$(p$	$\rightarrow_2$	$q)$
1	0	0∧1	0	1	0	0	1	0	0
2.°	4.°	5.°	2.°	0.°	3.°	0.°	1.°	0.°	1.°

Representando algunas fórmulas por sus juntores dominantes:

0.º, si $I(\rightarrow_1) = 0$, entonces $I(\rightarrow_0) = 1$ y $I(\rightarrow_2) = 0$;

1.º, $I(\rightarrow_2) = 0$ implica $I(p) = 1$ y $I(q) = 0$;

2.º, se propagan los valores $I(p)$ e $I(q)$ por toda la fórmula;

3.º, el valor de verdad de $\bot$ es 0;

4.º, como $I(\rightarrow_0) = 1$ y el valor de verdad de su consecuente ($\bot$) es 0, el de su antecendente (p) debe ser también 0;

5.º, de 2.º tenemos $I(p) = 1$ y $I(q) = 0$ —y, por tanto, $I(\neg q) = 1$— por lo que $I(p \wedge \neg q) = 1$; por otra parte, como $I(\wedge) = 0$ (de 4.º) e $I(p) = 1$, por definición del conjuntor, $I(\neg q) = 0$; de este modo, llegamos a $I(\neg q) = 1$ (por ser $I(q) = 0$) e $I(q) = 1$ (por ser $I(\neg q) = 0$), esto es, hemos alcanzado la fórmula insatisfactible $q \wedge \neg q$.

Como hemos derivado una fórmula insatisfactible a partir de suponer $\neg\mathcal{A}$, entonces, aplicando ahora reducción al absurdo (Abs, RAA), deducimos que $((p \wedge \neg q) \rightarrow \bot) \rightarrow (p \rightarrow q)$ es una fórmula válida, por lo que la inferencia $\mathcal{A}$ es válida y es admisible denominarla teorema (metalógico). ■

Observación 6.0.10.— Esto ha sido un mero ejemplo; insistimos en ello porque lo que es cierto es que hemos demostrado RAA usando RAA, lo cual no debemos hacer jamás en las matemáticas que estamos estudiando y con las que trabajaremos.

Observación 6.0.11.— En estos ejemplos también pudiésemos haber empleado otros procedimientos de decidibilidad, como las tablas de verdad[2] o las tablas analíticas/semánticas[3].

De seguro que es una buena actividad que intentemos solucionar cada uno de los ejemplos para así practicar todos los diferentes procedimientos que conoceremos al concluir el estudio del capítulo.

Ejemplo 224 Derivación formal como método de refutación

Demostremos que $\vdash p \wedge q \to p \vee q$.

Resolución.— Sea $A \leftrightharpoons p \wedge q \to p \vee q$.

Que A sea un teorema lógico es equivalente a que $\neg A$ sea inconsistente. Demostremos, pues, que $\{\neg A\} \vdash \bot$; en efecto:

0.	$\neg(p \wedge q \to p \vee q)$	Premisa
1.	$\neg(\neg(p \wedge q) \vee p \vee q)$	I 0 (Filón)
2.	$\neg(\neg p \vee \neg q \vee p \vee q)$	I 1 (De Morgan)
3.	$\neg(\neg p \vee p \vee \neg q \vee q)$	AD e I 2 (CoD)
4.	$\neg((\neg p \vee p) \vee (\neg q \vee q))$	AD 3
5.	$\neg(\top \vee \top)$	I 4 (I $\top$[PTE])
6.	$\neg\top$	I 5 (IdD)
7.	$\bot$	Defs. $\top$, $\bot$

I es la regla de intercambio.

Por tanto, al ser inconsistente $\neg A$, tenemos que A es un teorema lógico.

Observemos que lo que hemos hecho ha sido construir una derivación formal que *refuta* $\neg A$. ■

§ 6.1 Metalógica de la lógica de cuantores

[2] *Vid. supra* § 1.8 (pág. 124 de esta edición).
[3] *Vid. supra* § 3.3 (pág. 274 de esta edición).

§ 6.1.0 Consistencia, completitud y compacidad

La lógica de cuantores de primer orden es consistente.

Teorema 6.10 (Teorema de consistencia)
Para toda fórmula ϕ de la lógica de cuantores de primer orden, si ϕ es un teorema lógico, entonces ϕ es una fórmula válida.

Demostración.— De ser de nuestro interés, pudiésemos estudiarla, por ejemplo, en GARRIDO [64] (págs. 324–325). ■

Además, *la lógica de cuantores de primer orden es completa*, lo que demostró GÖDEL en 1930 ([108]).

Teorema 6.11 (Teorema de completitud —GÖDEL, 1930—)
Para toda fórmula ϕ de la lógica de cuantores de primer orden, si ϕ es válida, entonces ϕ es un teorema lógico.

Demostración.— HENKIN, en 1949 ([109]), y posteriormente HASENJAEGER, en 1952 ([110]), simplificaron la demostración de GÖDEL, de manera que este teorema surge como corolario del conocido actualmente como *teorema de satisfacción* de HENKIN.

De interesarnos, pudiésemos estudiar dichos teoremas y sus demostraciones, por ejemplo, en GARRIDO [64] (págs. 326–337). ■

Del teorema de satisfacción de HENKIN se sigue también el teorema de compacidad.

Teorema 6.12 (Teorema de compacidad)
Si Φ es un conjunto infinito de fórmulas tal que todo subconjunto finito suyo es satisfactible, entonces Φ es satisfactible.

Demostración.— De tener interés en ella, pudiésemos estudiarla, por ejemplo, en GARRIDO [64] (pág. 338). ■

§ 6.1.1 Decidibilidad de la lógica de primer orden con universo de referencia finito

La lógica de primer orden, monádica o poliádica, con universo de interpretación finito, es decidible.

Esto es así porque en tal caso, es posible sustituir los cuantores por expresiones lógicamente equivalentes en función de los juntores $\wedge$ y $\vee$. En efecto, si $a_0, a_1, \ldots, a_{n-1}$ son las entidades del universo, entonces[4]

$$\forall x Px \qquad \dashv\vdash Pa_0 \wedge Pa_1 \wedge \cdots \wedge Pa_{n-1}$$

[4] En la literatura, encontramos $\bigwedge$ y $\bigvee$ designando, respectivamente, los cuantores universal y existencial, debido, precisamente, a esta relación que existe entre los cuantores y los juntores en el caso finito.

$$
\begin{aligned}
\exists x Px &\dashv\vdash Pa_0 \lor Pa_1 \lor \cdots \lor Pa_{n-1} \\
\forall x \exists y Pxy &\dashv\vdash (Pa_0a_0 \lor Pa_0a_1 \lor \cdots \lor Pa_0a_{n-1}) \land \\
&\quad (Pa_1a_0 \lor Pa_1a_1 \lor \cdots \lor Pa_1a_{n-1}) \land \\
&\quad \cdots \land \\
&\quad (Pa_{n-1}a_0 \lor Pa_{n-1}a_1 \lor \cdots \lor Pa_{n-1}a_{n-1}).
\end{aligned}
$$

En otras palabras, en la lógica de primer orden, monádica o poliádica, con universo de interpretación finito, los cuantores no son más que *abreviaturas*.

Así, en dicha lógica, no es necesario el uso de cuantores, aunque se haga por comodidad, y demostrar la validez de una fórmula en esta lógica se reduce a demostrar la validez de dicha fórmula en lógica de juntores, cuestión que, como sabemos, puede resolverse, por ejemplo, mediante la construcción y comparación de la correspondiente tabla de verdad.

§ 6.1.2 Decidibilidad de la lógica de primer orden monádica

La lógica de primer orden monádica, sea cual sea su universo de referencia, es decidible.

En la interpretación corriente de la lógica bivalente,dado un universo $\mathcal{U}$ y una forma enunciativa Px, los valores de verdad (en realidad, conjuntos de valores de verdad) de ésta son:

- $\{1\}$ si todos los x de $\mathcal{U}$ satisfacen Px (Px es siempre verdadera);
- $\{0\}$ si ningún x de $\mathcal{U}$ satisface Px (Px es siempre falsa), y
- $\{0, 1\}$ en cualquier otro caso.

Esto asumiendo que en $\mathcal{U}$ siempre es posible asignar uno de tales valores de verdad a Px (si éste no fuese el caso, esto es, si supusiésemos que nuestro desconocimiento de Px es tal que no pudiésemos hacer ninguna de las asignaciones anteriores, deberíamos considerar la posibilidad de que su valor de verdad fuese $\emptyset$).

De este modo, los cuantores son aplicaciones, $\forall, \exists : 2^{\{0,1\}} \setminus \{\emptyset\} \longrightarrow \{0, 1\}$, pudiendo, entonces, construirse una tabla de verdad para ellos:

Px	$\forall x Px$	$\exists x Px$
$\{1\}$	1	1
$\{0, 1\}$	0	1
$\{0\}$	0	0

Puede hablarse entonces de *funciones de cuantificación*, que son $2^3 = 8$ en total.

Px	$\top xPx$	$\neg\forall xPx$	$\neg\exists^{\circ}xPx$	$\neg\exists xPx$	$\exists xPx$	$\exists^{\circ}xPx$	$\forall xPx$	$\bot xPx$
$\{1\}$	1	1	1	1	0	0	0	0
$\{0,1\}$	1	1	0	0	1	1	0	0
$\{0\}$	1	0	1	0	1	0	1	0
	$\neg\bot xPx$	$\exists x\neg Px$	$\neg\exists^{\circ}x\neg Px$	$\forall x\neg Px$	$\neg\forall x\neg Px$	$\exists^{\circ}x\neg Px$	$\neg\exists x\neg Px$	$\neg\top xPx$

donde,

- $\bot xPx$ es la *función cuantorial contradicción*, esto es, $\bot xPx$ puede ser interpretada, por ejemplo, como «todos los x de $\mathcal{U}$ satisfacen Px, aunque existe al menos un x de $\mathcal{U}$ que no satisface Px», es decir,
$$\bot xPx \longleftrightarrow (\forall xPx) \wedge (\exists x\neg Px), \tag{6.0}$$
- $\top xPx$ es la *función cuantorial tautología*, esto es, $\top xPx$ puede ser interpretada, por ejemplo, como «es falso que todos los x de $\mathcal{U}$ satisfagan Px y a la vez exista al menos un x de $\mathcal{U}$ que no satisfaga Px», es decir,
$$\top xPx \longleftrightarrow \neg((\forall xPx) \wedge (\exists x\neg Px)), \tag{6.1}$$
- $\exists^{\circ}$ es la *función cuantorial de existencia no global*, esto es, $\exists^{\circ}xPx$ significa que «existe algún x de $\mathcal{U}$ que satisface Px pero no todo x de $\mathcal{U}$ satisface Px», es decir,
$$\exists^{\circ}xPx \longleftrightarrow (\exists xPx) \wedge (\neg\forall xPx). \tag{6.2}$$

Además de (6.0), (6.1) y (6.2), comparando la cabecera y el pie del cuadro anterior apreciamos las interdefiniciones entre $\forall$ y $\exists$, esto es,
$$\exists xPx \longleftrightarrow \neg\forall x\neg Px$$
$$\forall xPx \longleftrightarrow \neg\exists x\neg Px$$
por lo que basta con asumir un único cuantor, $\forall$ o $\exists$, como primitiva de todas las funciones de cuantificación.

Recordemos que el cuantor de existencia única no pertenece a la lógica de cuantores sino a la lógica de primer orden con identidad[5], sin embargo, para nuestro quehacer lógico-matemático es útil y cómodo. Por ejemplo, la afirmación «de existir algún x que satisfaga Px, no habría más de uno» pudiese expresarse como
$$(\forall x\neg Px) \vee (\exists! xPx).$$

[5] *Vid. supra* § 5.6.0 (pág. 423 de esta edición).

Ejemplo 225

Demostremos mediante una tabla de verdad la equivalencia entre $\forall x \neg Px$ y $\neg \exists x Px$.

Resolución.— Observando su tabla de verdad,

Px	$\forall x$	$\neg Px$	$\boxed{\rightarrow}$	$\neg$	$\exists x Px$
$\{0\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{0\}$
$\{0,1\}$	$\{0\}$	$\{0,1\}$	$\{1\}$	$\{0\}$	$\{1\}$
$\{1\}$	$\{0\}$	$\{0\}$	$\{1\}$	$\{0\}$	$\{1\}$

vemos que la fórmula $\forall x \neg Px \leftrightarrow \neg \exists x Px$ es válida. ■

Ejemplo 226

¿Es válida la argumentación «Toda persona que deja que otra piense por ella, dejará que otra piense por ella o que también lo haga un artefacto»?

Resolución.— Formalizando: $Px \leftrightharpoons x$ deja que otra piense por ella; $Qx \leftrightharpoons x$ deja que un artefacto piense por ella, y siendo el dominio de interpretación las personas ¿Es válida $\forall x(Px \rightarrow Px \vee Qx)$?

Px	Qx	Px	$\rightarrow$	$Px \vee Qx$	$\boxed{\forall x\,(Px \rightarrow Px \vee Qx)}$
$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	1
$\{1\}$	$\{0\}$	$\{1\}$	$\{1\}$	$\{1\}$	1
$\{1\}$	$\{0,1\}$	$\{1\}$	$\{1\}$	$\{1\}$	1
$\{0,1\}$	$\{1\}$	$\{0,1\}$	$\{1\}$	$\{1\}$	1
$\{0,1\}$	$\{0\}$	$\{0,1\}$	$\{1\}$	$\{0,1\}$	1
$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{1\}$	$\{0,1\}$	1
$\{0\}$	$\{1\}$	$\{0\}$	$\{1\}$	$\{1\}$	1
$\{0\}$	$\{0,1\}$	$\{0\}$	$\{1\}$	$\{0,1\}$	1
$\{0\}$	$\{0\}$	$\{0\}$	$\{1\}$	$\{0\}$	1

En las filas enmarcadas, las implicaciones $\{0,1\} \rightarrow \{0,1\}$ son verdaderas; basta observar que las evaluaciones se hacen para un x determinado, el mismo para Px y para $Px \vee Qx$. La única posibilidad de que tales implicaciones fuesen falsas es si Px es 1 y $Px \vee Qx$ es 0, pero esto, por definición de disyunción, es imposible. ■

Aunque aparentemente las tablas veritativas funcionan en el caso de la lógica de primer orden monádica, puede surgirnos la duda de su aplicabilidad general y por tanto de la decidibilidad de dicha lógica.

Fue LÖWENHEIM [111], en 1915, quien demostró que la lógica de primer orden monádica es decidible. Lo hizo reduciendo el problema de decibilidad a un dominio de interpretación finito, esto es, que para demostrar que una fórmula de la lógica de primer orden monádica es válida, basta demostrarlo en un dominio finito, en concreto de 2^n entidades, siendo n el número de predicados de la fórmula.

Teorema 6.13 (Teorema de decidibilidad de LÖWENHEIM, 1915)
Si una fórmula de la lógica de primer orden monádica, que consta de n predicados distintos, es válida en un dominio de interpretación de al menos 2^n objetos, entonces es válida en todo dominio de interpretación no vacío, sea finito o no.

Demostración.— De ser de nuestro interés, pudiésemos estudiarla, por ejemplo, en GARRIDO [64] (págs. 346–347). ■

En teoría, perfecto, pero en la práctica se necesitaría una tabla de verdad enorme para determinadas fórmulas. En vez de tal teorema se utilizan ciertos algoritmos —*cfr. v. gr.* FROST (1989) y GARRIDO [64] (págs. 347ss.).

§ 6.1.3 Semidecidibilidad de la lógica de primer orden poliádica

La lógica de cuantores de primer orden poliádica no es decidible, si bien es parcialmente decidible, es decir, existen subcolecciones de fórmulas para las que sí se tiene la decidibilidad.

Análogamente a lo que hicimos en § 6.1.2 (pág. 453 de esta edición), es posible explorar la posibilidad de aplicar el método de las tablas veritativas a los cuantores en relación con los valores de verdad de una forma enunciativa.

En el caso diádico, por ejemplo, dados dos referenciales $\mathcal{U}_0$ y $\mathcal{U}_1$ y dada una forma enunciativa Pxy, los valores de verdad de ésta son:

- $\{1\}$ si cualquier pareja $\langle x, y\rangle \in \mathcal{U}_0 \times \mathcal{U}_1$ satisface Pxy (Pxy es siempre verdadera);
- $\{0\}$ si ninguna pareja $\langle x, y\rangle \in \mathcal{U}_0 \times \mathcal{U}_1$ (Pxy es siempre falsa), y
- $\{0, 1\}$ en cualquier otro caso.

Los cuantores son aplicaciones, $\forall, \exists : 2^{\{0,1\}} \setminus \{\emptyset\} \longrightarrow 2^{\{0,1\}} \setminus \{\emptyset\}$, pudiendo, entonces, construirse una tabla de verdad para ellos (el caso monádico queda incluido identificando 0 y 1 con $\{0\}$ y $\{1\}$, respectivamente):

Pxy	$\forall x\forall yPxy$	$\forall x\exists yPxy$	$\forall y\exists xPxy$	$\exists y\forall xPxy$	$\exists x\forall yPxy$	$\exists x\exists yPxy$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
$\{0,1\}$	$\{0\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{1\}$
$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$

Ejemplo 227

¿Es válida $\forall x \exists y Pxy \to \exists x \exists y Pxy$?

Resolución.— Observando su tabla de verdad,

Pxy	$\forall x \exists y Pxy$	$\boxed{\to}$	$\exists x \exists y Pxy$
$\{0\}$	$\{0\}$	$\{1\}$	$\{0\}$
$\{0,1\}$	$\{0,1\}$	$\{1\}$	$\{1\}$
$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$

vemos que la fórmula es válida. ∎

Aunque pudiese parecernos que este camino asegura la decidibilidad, no es así.

Fue Alonzo CHURCH en 1936 ([112]) —independientemente, TURING, 1937 ([113])— quien demuestra que la lógica de primer orden es indecidible (a pesar de que una parte suya, la monádica, sí es decidible). Lo que sí ocurre es que se conocen varios tipos de fórmulas poliádicas decidibles, de entre las cuales Manuel GARRIDO [64] (págs. 348–349) destaca tres —descubiertas ya por BERNAYS y SCHÖNFINKEL en 1928 ([114])—, dado que hayan sido reducidas previamente a forma normal prenexa (FNP) (aquella fórmula en que todos los cuantores están al principio de ella)[6]:

- todas las fórmulas del tipo $\forall x_0 \dots \forall x_i \exists x_{i+1} \dots \exists x_{n-1} P x_0 \dots x_{n-1}$;
- todas las fórmulas del tipo $\forall x_0 \dots \forall x_{n-1} P x_0 \dots x_{n-1}$;
- todas las fórmulas del tipo $\exists x_0 \dots \exists x_{n-1} P x_0 \dots x_{n-1}$.

§ 6.2 Sobre la metalógica de algunas extensiones

Para la extensión aritmética de la lógica de primer orden[7], se demuestra que no existe ningún procedimiento decisorio para determinar sus teoremas ni que puedan ser efectivamente enumerados.

Así:

- la aritmética, la «simple» aritmética con igualdad, suma y producto en los naturales, no es decidible (Alfred TARSKI y Andrzej MOSTOWSKI, 1949);
- tampoco lo es la aritmética racional con igualdad, suma y producto (Julia ROBINSON, 1949);

[6] *Vid. supra* § 5.5 (pág. 420 de esta edición).
[7] *Vid. supra* § 5.6.2 (pág. 429 de esta edición).

- pero sí lo es la aritmética real (lo que implica que no exista ninguna fórmula en el lenguaje de la estructura de los números reales que defina los números naturales);
- de hecho, es decidible la aritmética de cualquier cuerpo real cerrado (Alfred TARSKI, 1949).

También se tiene que:

- las teorías de las álgebras de BOOLE es decidible (Alfred TARSKI, 1940);
- las teorías de los órdenes totales y de los órdenes buenos son decidibles;
- pero si bien la teoría de una relación de equivalencia es decidible,
- la de dos relaciones de equivalencia —todas las aseveraciones que pueden deducirse del hecho de tener dos relaciones de equivalencia— no lo es;
- tampoco lo es la teoría de una relación de similitud (compatibilidad, tolerancia, relación reflexiva y simétrica).

Y también que:

- la teoría de una función de un argumento es decidible,
- pero la de dos funciones de un argumento no lo es;
- tampoco lo es la teoría de una función diádica (dos argumentos);
- sí lo son, en cambio, las teorías de dos funciones sucesor, de un número finito de funciones sucesor y de un número numerable de funciones sucesor.

Además,

- mientras que la teoría de grupos no es decidible (Alfred TARSKI, 1953),
- la teoría de los grupos abelianos —es decir, el conjunto de aseveraciones en el lenguaje de la teoría de grupos que son verdaderas para los grupos abelianos— es decidible (Wanda Montlak SZMIELEW, 1955);
- las teorías de grupos finitos, semigrupos y anillos tampoco son decidibles (Anatoly Ivanovich MAL'CEV, 1961);
- la teoría de cuerpos tampoco lo es (Julia ROBINSON, 1949).

Se han descrito muchas extensiones, formalizado clases enteras de lenguajes y estudiado sus interrelaciones y su relación con las diferentes aritméticas y estructuras y se sigue haciendo. El estudio se amplía a lógicas de órdenes superiores, esto es, donde las variables representan no sólo a entidades, sino a relaciones y metarrelaciones de cualesquiera aridades. Aquí, de nuevo, las cosas pueden cambiar; a modo de ejemplo, la teoría de primer orden en $(\mathbb{N}; <)$ es decidible pero la de segundo orden no lo es.

La matemática, la filosofía y la física cuántica, junto al afán de simular e incluso crear inteligencia y conciencia[8], impulsan el continuo estudio de los límites de lo computable.

Metaprogramación

Un concepto en cierto sentido y en cierto grado similar al de metalógica es el de *metaprogramación*: programas que se modifican, se clonan, o modifican o crean otros programas —para lo que tienen que analizarlos para conocer sus estructuras, propiedades, intrínsecas y de interacción—; no sólo software, más allá, un mundo de *máquinas autorreplicantes*, y aún más allá, individuos del *Machina sapiens* capaces de replicarse en una forma mejorada. Pudiese ser interesante tomar como puntos de partida la lectura de *Self-replicating machine*[*] y alguna acerca de *Core War*, por ejemplo, *Core War - the Ultimate Programming Game*[†].

[*] https://en.wikipedia.org/wiki/Self-replicating_machine.
[†] https://corewar.co.uk/.

§ 6.3 Bibliografía

- Para una primera aproximación:

  [62] María Manzano Arjona y Antonia Huertas Sánchez. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

  [99] Amador Antón Antón y Pascual Casañ Muñoz. *Lógica matemática. II. Lógica de predicados*. NAU llibres, Valencia, España, 1998.

- Para estudiar, practicar y conocer más:

  [64] Manuel Garrido Giménez. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

  [65] Carmen García Trevijano. *El arte de la lógica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1999.

- Para profundizar, acullá:

  [66] Manuel Garrido Giménez, Luis Manuel Valdés Villanueva, Jesús Mosterín de las Heras, Alfonso García Suárez y Carlos-Peregrín Fernández Otero. *Lógica y lenguaje*. Cuadernos de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1989.

  [67] Raymond Merrill Smullyan. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

[8] *Vid. infra* Conciencia de la autoconciencia (pág. 512 de esta edición).

[60] Herbert Bruce ENDERTON. *A mathematical introduction to logic*. Harcourt/Academic Press, San Diego, Condado de San Diego, California (US-CA), Estados Unidos de América, 2.ª ed., 2001.

Capítulo 7

De la demostración

It's not what you know. It's what you can prove [No se trata de lo que sabes sino de lo que puedes demostrar].

(Alonzo Harris [Denzel Washington], *Training Day* [Día de entrenamiento] <https://www.imdb.com/title/tt0139654/quotes>).

«*Felix qui potuit rerum cognoscere causas*! [¡Feliz quien ha podido conocer las causas de las cosas!]» (Virgilio). En cualquier caso, la diversidad de estrategias en sí misma es una estrategia, o una metaestrategia, como prefiramos llamarla, necesitada, no obstante, de la salvaguarda de la precisión en nuestros objetivos y la dedicación de nuestros mayores esfuerzos en conseguirlos.

§ 7.0 Heurística

A la hora de resolver una cuestión matemática, debiésemos recorrer las tres *etapas* siguientes:

0. *conceptualización*, o traducción de la realidad a un modelo matemático;

1. *razonamiento lógico-deductivo* para llegar a la solución del problema;

2. *desconceptualización*, o aplicación de la solución al problema real del que partimos.

George Pólya [115] propuso las siguientes *reglas básicas heurísticas* «Para resolverlo»:

A. comprendamos el problema;

B. averigüemos qué conexiones hay entre los datos y las incógnitas; de no ser posible hallar conexiones inmediatas, pudiese ser necesario que examinásemos problemas auxiliares; al final, deberíamos obtener un plan de resolución;

C. llevemos a efecto nuestro plan;

D. examinemos la solución obtenida.

Pólya descompone cada una de estas reglas, sugiriendo *estrategias individuales* a las que pudiésemos recurrir en momentos adecuados:

I. si no es posible resolver el problema propuesto, busquemos un problema similar apropiado, que sí sepamos resolver;

II. demos el problema por resuelto, y tratemos de desandar el camino;

III. tratemos de avanzar;

IV. restrinjamos las condiciones;

V. relajemos las condiciones;

VI. busquemos un contraejemplo;

VII. tanteemos;

VIII. dividamos y venceremos;

IX. cambiemos el enfoque conceptual.

Ni qué decir tiene que investigadores posteriores han desarrollado las ideas de Pólya de diversos modos —Schoenfeld en 1979 ([116]), vía Davis y Hersh en 1989 ([117]); Mason, Burton y Stacey en 1989 ([118])—:

La práctica de estas heurísticas y otras que busquemos, contrastemos y adquiramos, probablemente contribuirá a que tomemos conciencia de los siguientes *puntos fundamentales* (*cfr.* Mason, Burton y Stacey [118]).

- somos capaces de pensar matemáticamente, no sólo cada persona por sí misma, también la sociedad desde su inteligencia colectiva;
- el razonamiento matemático puede mejorarse por la práctica unida a la reflexión;
- el razonamiento matemático viene motivado por un desafío, o una sorpresa, o una contradicción, o el descubrimiento de un vacío de comprensión;
- el razonamiento matemático se mueve en una atmósfera de interrogantes, desafíos y reflexión, con abundante tiempo y espacio;
- el razonamiento matemático nos ayudará a entendernos mejor, cada persona a sí misma y a la sociedad, logrando una visión más consistente de lo que sabemos y una investigación más eficaz de lo que queremos saber, así como a un mejor conocimiento del mundo que nos rodea, lo cual nos hará adoptar una postura más crítica.

El hecho de que no tengamos un problema fijo a resolver, sino una situación abierta, con posibilidades de hacer descubrimientos, pudiese provocarnos un desconcierto inicial, que es superable, y, aún más, debe serlo. Al conseguirlo, experimentaremos una sensación de alborozo y libertad y de control de la materia que estemos estudiando.

El enunciado de la cuestión matemática; el blanco que sigue en la página; a la hora de enfrentarnos a esto, *en nuestra práctica*:

a. *analicemos* la cuestión;

b. *averigüemos* el camino más adecuado para conseguir su resolución;

c. *diseñemos* cómo recorrer dicho camino, explicitando las fases, etapas o pasos a seguir;

d. *codifiquemos* este recorrido en el lenguaje lógico-matemático;

e. *documentemos* narrativamente esta codificación;

f. *revisemos* esta codificación y su documentación.

Ejemplifiquemos a continuación algunas de las estrategias anteriores.

§ 7.0.0 La estrategia de tanteo (ensayo y error)

La estrategia de tanteo (o, sinónimamente, de ensayo y error) —*cfr. supra* Pólya, VII— consiste en comenzar probando con una o más entidades del dominio, según lo que estemos investigando; si se satisface lo buscado, hemos terminado, de lo contrario, seguiríamos probando con otras.

Ejemplo 228

En el sistema decimal, ¿existe alguna pareja de números primos de dos cifras, xy e yx (permutado del anterior), tales que su suma es un número capicúa?

Resolución.— Sin más información, elijamos uno al azar, por ejemplo, 23; para él no se satisface, pues su permutado, 32, no es primo.

Probemos con 17: $17 + 71 = 88$; pues sí que se satisface, 88 es un número capicúa. ■

§ 7.0.1 La estrategia de la sencillez

A falta de información, comenzamos analizando los casos más sencillos.

Ejemplo 229

En el ejemplo anterior, ¿no hubiese sido mejor comenzar por un número relacionado con lo que se pregunta que por uno aleatorio?

Resolución.— En efecto, ¿por qué hemos comenzado analizando el número 23 y después el 17? ¿Por qué no hemos comenzado por el menor número que satisfacía los requisitos, el 11? Es más, si hubiésemos comenzado por él, el ensayo habría sido exitoso: $11+11 = 22$ (capicúa) (analizar el número 11 es válido, pues no se exige que los primos xy e yx deban ser distintos). ■

§ 7.0.2 La estrategia de la sistematicidad

Que el análisis siga un sistema, método u orden tiene sus ventajas. Bien comenzar con los casos más sencillos pasando gradualmente a casos más difíciles si la cuestión así lo requiere, bien comenzar con los casos de los que se tenga algo de información.

Ejemplo 230

Sirva de ejemplo el análisis progresivo a la hora de resolver ecuaciones en diferencias.

§ 7.0.3 La estrategia regresiva

Esta estrategia —*cfr. supra* PÓLYA, II— consiste en dar el problema por resuelto y desandar el camino.°

Ejemplo 231

Sirva de ejemplo el análisis regresivo a la hora de resolver ecuaciones en diferencias.

§ 7.1 La cuestión de la existencia

Para *demostrar la existencia* de al menos una entidad en un universo dado que satisface en él una propiedad determinada, disfrutamos de varias posibilidades:

- proporcionar un argumento válido cuya conclusión sea la existencia de tal entidad —*estrategia no constructiva*—;
- proporcionar un camino para encontrar dicha entidad, pero que debido a la dificultad técnica del mismo no sea posible con la matemática conocida;
- encontrar dicha entidad, mediante un camino conocido o que tracemos o sin él, por puro azar;
- construir, fabricar, generar dicha entidad —*estrategia constructiva*—, en definitiva, crearla.

Ejemplo 232

¿Cómo pudiésemos demostrar que un conjunto finito es no vacío?

Resolución.— Como un conjunto finito tiene un número par o impar de elementos, si consiguiésemos demostrar que tiene un número impar de elementos, ya habríamos demostrado que es no vacío, pues al menos tendría un elemento (el primer impar positivo). ■

Cfr. infra § 7.5 (pág. 469 de esta edición) (la estrategia del ejemplo).

Para *demostrar la no existencia* de ninguna entidad de un universo que satisface una propiedad determinada debemos demostrar que toda entidad de tal universo no satisface dicha propiedad. Esto es una aplicación de la regla de interdefinición Negación del generalizador (NG), $\neg\exists Px \dashv\vdash \forall x \neg Px$.

° Podemos ver un ejemplo con un grado de abstracción mucho más allá de estas notas, incluso de sus márgenes, en https://plato.stanford.edu/entries/reverse-mathematics/.

Ejemplo 233

En el sistema decimal, hallemos dos números primos de dos cifras, xy e yx, tales que las cifras de su suma estén en progresión aritmética de diferencia 1.

Resolución.— Hay 21 números primos de dos cifras, a saber: 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

Con una primera inspección observamos cómo los permutados de los números $2y$, $4y$, $6y$ y $8y$ son pares, esto es, no son primos, y tampoco lo son los permutados de $5y$ (por ser $y5$ múltiplo de 5), por lo que sólo hemos de analizar: 11, 13, 17, 19, 31, 37, 71, 73, 79 y 97.

Con una segunda inspección, simplificamos, quedándonos con sólo uno de cada par de permutados, en definitiva: 11, 13, 17, 19, 37 y 79.

Veamos, pues:

$11 + 11 = 22$, no, pues 2, 2 no están en progresión aritmética de diferencia 1;
$13 + 31 = 44$, no, pues 4, 4 no están en progresión aritmética de diferencia 1;
$17 + 71 = 88$, no, pues 8, 8 no están en progresión aritmética de diferencia 1;
$19 + 91 = 110$, no, pues 91 no es primo;
$37 + 73 = 110$, no, pues 1, 1, 0 no están en progresión aritmética de diferencia 1;
$79 + 97 = 176$, no, pues 1, 7, 6 no están en progresión aritmética de diferencia 1. ■

§ 7.2 La cuestión de la unicidad

Para *demostrar la unicidad*, esto es, que existe exactamente una entidad que satisface una propiedad determinada, pudiésemos seguir la siguiente estrategia:

0.º consideramos dos entidades cualesquiera x e y que satisfagan la propiedad;

1.º demostramos que necesariamente $x = y$, y

2.º concluimos que sólo existe una entidad que satisface la propiedad y que lo único que ha ocurrido es que nos hemos referido a ella con dos nombres distintos (x e y).

Para *demostrar la no unicidad*, debemos encontrar al menos dos entidades distintas que satisfagan la propiedad dada.

§ 7.3 Demostrar un teorema matemático

Dada la corrección y consistencia de la lógica de primer orden, en la matemática,

- las deducciones formales, $\Phi \vdash A$ y las implicaciones lógicas, $\Phi \vDash A$, «colapsan» en *implicaciones matemáticas*, $\Phi \Rightarrow A$, y
- las deducciones formales mutuas, $\Phi \dashv\vdash A$ y las equivalencias lógicas, $\Phi \equiv A$, colapsan en *equivalencias matemáticas*, $\Phi \Leftrightarrow A$.

Observación 7.3.0.— El concepto de implicación matemática puede entenderse ampliamente como el de *inferencia matemática*[1].

Observación 7.3.1.— Recordemos que los signos $\therefore$ («luego/por lo tanto») y $\because$ («debido a/porque») se sitúan en el grado metalingüístico de la lengua natural, siendo sus correspondientes en el lenguaje (lógico-)matemático precisamente $\Rightarrow$ y $\Leftarrow$, respectivamente.

Demostrar $A \Leftrightarrow B$ equivale a demostrar que se satisfacen $A \Rightarrow B$ y $B \Rightarrow A$.

. . . .

A continuación veremos algunas estrategias para demostrar la validez o falsedad de un *teorema matemático*, esto es, una forma matemática $A \Rightarrow B$. Como tales estrategias proceden de la lógica de primer orden, usaremos $\rightarrow$, $\leftarrow$ y $\leftrightarrow$ en vez de $\Rightarrow$, $\Leftarrow$ y $\Leftrightarrow$, respectivamente, designando un teorema matemático por $A \rightarrow B$.

. . . .

§ 7.4 La estrategia de la vacuidad

Consideremos un universo vacío. Ninguna entidad en él. La *estrategia de la vacuidad* se basa en la imposibilidad de demostrar la negación de lo afirmado, precisamente por la inexistencia de entidades en el universo.

Por ejemplo, pudiésemos afirmar que todas las entidades satisfacen (resp., ninguna entidad satisface) la propiedad P, ¿o acaso pudiésemos encontrar alguna entidad que no satisfaga (resp., satisfaga) la propiedad P?

Pensemos en la pregunta que actúa como respuesta a la primera como la acción de una ley de De Morgan sobre aquélla, pues si, en notación de Dijkstra[2] afirmamos $\forall(x : \emptyset : Px)$, para demostrar su falsedad, es decir, que $\neg\forall(x : \emptyset : Px)$, debiésemos demostrar la veracidad de $\exists(x : \emptyset : \neg Px)$ [por la ley de De Morgan], esto es, debiésemos ser capaces de encontrar en $\emptyset$ un elemento x que satisficiese $\neg Px$, pero dado que no hay elementos en $\emptyset$, encontrarlo es imposible, luego afirmar que podemos hacerlo es falso, luego lo cierto es que $\forall(x : \emptyset : Px)$.

[1] *Cfr. supra* § 5.7 (pág. 432 de esta edición).
[2] *Vid. supra* § 5.6.2 (pág. 429 de esta edición).

Pero, ¿pudiésemos afirmar que alguna entidad satisface (resp., no satisface) la propiedad P? No, como no hay elementos en $\emptyset$, afirmar que podemos encontrar en $\emptyset$ un elemento x que satisfaga Px (resp., $\neg Px$) es simplemente falso.

En resumen: $\forall(x : \emptyset : Px) \equiv \top$ y $\exists(x : \emptyset : Px) \equiv \bot$.

§ 7.5 La estrategia del ejemplo

La *estrategia del ejemplo* la usamos cuatro subcapítulos atrás para resolver una cuestión de existencia[3] y todo consiste en encontrar un ejemplo que satisfaga la propiedad en estudio.

Ejemplo 234

¿Cómo demostraríamos la afirmación de que en una bolsa determinada hay alguna bola blanca?

Resolución.— Bastaría encontrar una bola blanca en la bolsa para demostrar la validez de lo afirmado. ■

§ 7.6 La estrategia constructiva

Usar la *estrategia de la construcción* significa proporcionar un procedimiento de creación, construcción, fabricación, generación, de una entidad que satisfaga la afirmación a demostrar.

Ejemplo 235

Si $|x-a| < b$, acotemos inferior y superiormente x, esto es, hallemos k y k', reales, tales que $k < x < k'$.

Resolución.— Veamos cómo construimos valores adecuados para k y k'. Suponiendo $b > 0$ para que tenga solución, entonces, por definición de valor absoluto, $|y| = y$ si $y \geq 0$, $|y| = -y$ si $y < 0$, por lo que $|y| < b$ es $y < b$ si $y \geq 0$, $-y < b$ si $y < 0$, esto último es, $-b < y$ si $y < 0$, en definitiva, sólo dos opciones, $-b < y$ o $y < b$, abreviadamente, $-b < y < b$. Tomando ahora $y = x - a$, $|x - a| < b$ equivale a $-b < x - a < b$, de donde, sumando a los tres miembros a, $a - b < x < a + b$; por lo tanto, una cota inferior es $k = a - b$ y una cota superior es $k' = a + b$; resumiendo, si $b > 0$: $|x - a| < b$ si, y sólo si, $a - b < x < a + b$. ■

[3] *Cfr. supra* § 7.1 (pág. 466 de esta edición).

Ejemplo 236

Hallemos la ecuación en $\mathbb{R}$ de un punto x del segmento $[p, q]$ en función de p y q.

Resolución.— Veamos cómo construimos dicha ecuación. La ecuación vectorial de la recta que pasa por los puntos $(p, 0)$ y $(q, 0)$ es $(x, y) = (p, 0) + t(q - p, 0)$, $t \in \mathbb{R}$; de ella, $x = p + t(q - p)$, $t \in \mathbb{R}$, esto es, $x = (1 - t)p + tq$, $t \in \mathbb{R}$; de aquí que la ecuación paramétrica del segmento en $\mathbb{R}$ sea $x = (1 - t)p + tq$, $t \in [0, 1]$ (una combinación lineal convexa de p y q). ■

Observación 7.6.0.— Esto se extiende fácilmente a más dimensiones; por ejemplo, las coordenadas de un punto X del segmento PQ, donde P y Q son dos puntos del plano, de coordenadas (x_P, y_P) y (x_Q, y_Q) son $((1 - t)x_P + tx_Q, (1 - t)y_P + ty_Q)$, con $t \in [0, 1]$. Claro que si, por ejemplo, lo que nos interesase fuesen las coordenadas de cualquier punto X del cuadrado relleno (una bola cerrada según d_∞) de diagonal el segmento PQ, tendríamos que utilizar dos parámetros: $((1 - \alpha)x_P + \alpha x_Q, (1 - \beta)y_P + \beta y_Q)$, con $\alpha, \beta \in [0, 1]$.

Otra cosa es que hubiésemos buscado y encontrado o incluso construido uno o más ejemplos que satisfagan un teorema con la pretensión de demostrarlo; en general, esto no tiene por qué demostrar la validez del teorema; sí sucederá así, sin embargo, cuando el universo sea finito[4] o el teorema sea existencial[5]. Y otra es que estuviésemos embarcados en la demostración de la no validez de un teorema, en este caso sí bastaría con encontrar un ejemplo de su negación, como vemos en el subcapítulo que sigue.

§ 7.7 La estrategia del contraejemplo

Si sospechamos que no es correcto el teorema matemático $A \to B$, pudiésemos demostrar este hecho encontrando un ejemplo para su negación, esto es, donde A sea verdadera y B sea falsa, en definitiva, hallando un modelo para $\{A, \neg B\}$. Decimos entonces que hemos encontrado un *contraejemplo* al teorema.

Observemos que un único contraejemplo es suficiente para demostrar la invalidez del teorema. Sin embargo, el hecho de que no encontremos un contraejemplo no significa que el teorema sea válido.

Ejemplo 237

¿Es válido afirmar que todos los libros están dedicados a la matemática?

[4] *Cfr. infra* § 7.13.5 (pág. 479 de esta edición) (la estrategia de la prueba por casos).
[5] *Cfr. supra* § 7.5 (pág. 469 de esta edición) (la estrategia del ejemplo).

Resolución.— Su expresión en lógica de primer orden es $\forall x(\text{Libro}(x) \rightarrow \text{LibDedMat}(x))$. Su negación es $\exists x(\text{Libro}(x) \wedge \neg\text{LibDedMat}(x))$. En efecto, existe un libro, por ejemplo, El Quijote, que no está dedicado a la matemática. ■

§ 7.8 La estrategia de la analogía

Identificamos el problema como análogo a otro que sabemos demostrar.

Por ejemplo, cuando estudiemos combinatoria[6], trabajaremos con cuatro modelizaciones: modelización I, selección de muestras y etiquetado de unidades con y sin repetición; modelización II, agrupamiento de unidades (distribución, almacenamiento o colocación de objetos en recipientes); modelización III, partición de conjuntos y de multiconjuntos, y modelización IV, partición (descomposición aditiva) de un entero positivo. Ellas nos servirán para modelizar cuatro problemas combinatorios de recuento simples y otras operaciones combinatorias.

§ 7.9 La estrategia de la reducción

Reducir a un problema más general que sabemos demostrar, esto es, el problema entre manos es un caso particular del que ya conocemos.

§ 7.10 La estrategia de la reformulación

Reformular el problema a formas enunciativas equivalentes de menor complejidad (o de mayor complejidad, si esto propicia una vía de solución).

Por ejemplo, cuando pensamos en las estrategias anteriores de analogía y reducción, la reformulación está presente: reformulamos el problema en los términos del análogo o del general, respectivamente.

Esta estrategia la hemos aplicado en lógica de primer orden: en las simplificaciones por equivalencias lógicas; en la traducción directa (del lenguaje de la lógica al español) (L1 a L0) (desconceptualización), y también en la traducción inversa (del español al lenguaje de la lógica) (L0 a L1) (conceptualización).

Asimismo, en algunos ejemplos y actividades no instrumentales de las diferentes materias estudiadas.

[6] *Cfr. infra* § 19 (pág. 1124).

Ejemplo 238

¿Sabríamos resolver la ecuación $\sqrt{x+\sqrt{x+2}}=2$?

Resolución.— Reformulemos la cuestión a una forma enunciativa más compleja por sustitución, pero que nos proporcionará su resolución. Veamos. Sustituimos el 2 interior por su valor según esa ecuación:

$$\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+2}}}}=2,$$

y repetimos esta sustitución,

$$\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+2}}}}}}=2,$$

una y otra vez,

$$\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+\sqrt{x+2}}}}}}}}=2,$$

así, sucesivamente, infinitas veces, lo que abreviadamente expresamos como

$$\sqrt{x+\sqrt{x+\sqrt{x+\dots}}}=2,$$

y como $\infty-1=\infty$, esta última ecuación es equivalente a[7]

$$\sqrt{x+2}=2,$$

de donde $x=2$. ■

[7] Abstraemos la infinidad de raíces como ∞ y utilizamos ∞ como un simple instrumento: $\infty-1=\sqrt{x+\sqrt{x+\sqrt{x+\dots}}}-\sqrt{x+2}=\sqrt{x+\sqrt{x+\sqrt{x+\dots}}}-2=\infty-2$.

§ 7.11 La estrategia visual

Pudiésemos distinguir entre:

- como apoyo a una estrategia no visual, sea escrita u oral;[8]
- puramente visual (o de *álgebra geométrica*), sin palabras, sea una imagen estática, un fotograma o una película.[9]

§ 7.12 La estrategia diagramática

Sería posible considerarla también como un caso particular o al menos entroncado con la estrategia visual.

Tenemos un ejemplo de su utilización, en estas notas, justo el ejemplo 100 (pág. 148 de esta edición).

§ 7.13 Las estrategias fundamentadas en reglas deductivas

Cada una de las reglas deductivas[10] fundamenta una estrategia de demostración.

A modo de ejemplo, veamos las siguientes.

§ 7.13.0 La estrategia del *modus ponens*

Comúnmente llamada *demostración directa*. Esta estrategia corresponde a la regla de inferencia deductiva *modus ponendo ponens*, esto es, $A \to B, A \vdash B$. Por tanto, lo que nos preocupa es demostrar $A \to B$ para después inferir B de A vía dicha regla.

Ejemplo 239

De ser un número entero múltiplo de 10, ¿es posible deducir que es múltiplo de 5?

Resolución.— Sí. Por una parte, demostremos que $(\forall x \in \mathbb{Z})(10 | x \to 5 | x)$; en efecto, que 10 divida a x equivale a que $(\exists k \in \mathbb{Z})(x = k \cdot 10)$, lo que equivale a su vez a que $(\exists k \in \mathbb{Z})(x = k \cdot 2 \cdot 5)$, de donde, como $k \cdot 2 \in \mathbb{Z}$, se sigue que $(\exists h \in \mathbb{Z})(x = h \cdot 5)$, ya que $k \cdot 2$ sirve como ejemplo de un tal h.

---

[8] *Cfr. v. gr.* Guzmán [119].

[9] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Demostraci%C3%B3n_sin_palabras. (Recordemos que las páginas en diferentes lenguas no son intertraducciones por lo que es recomendable consultar todas de las que podamos prevalernos).

[10] *Cfr. supra* § 2.2 (pág. 190ss. de esta edición).

Por otra, consideremos un $x \in \mathbb{Z}$ tal que $10 \mid x$.

Entonces por *modus ponens*, obtenemos que $5 \mid x$. ■

§ 7.13.1 La estrategia del *modus tollens*

Comúnmente llamada *demostración indirecta*. Este método corresponde a *modus tollendo tollens*, esto es, $\neg A \to B, \neg B \vdash \neg\neg A$, de donde se sigue A por la involutoriedad de $\neg$.

Por tanto, lo que nos preocupa es demostrar $\neg A \to B$ para después inferir A de $\neg B$ vía *modus tollens*.

Ejemplo 240

De ser un número entero múltiplo de 10, ¿es posible deducir que es múltiplo de 5?

Resolución.— Designemos «x es múltiplo de 5» por A y «x no es múltiplo de 10» por B. No es difícil demostrar que $\neg A \to B$ —*cfr. infra* ejemplo 241 (pág. 474 de esta edición)—.

Por otra, sea $x \in \mathbb{Z}$ tal que x es múltiplo de 10, esto es, $\neg B$.

Entonces por *modus tollens*, obtenemos A, esto es, que x es múltiplo de 5. ■

§ 7.13.2 La estrategia de la contraposición

Esta estrategia corresponde a la Ley de Contraposición (Cp)[11], esto es, $(A \to B) \dashv\vdash (\neg B \to \neg A)$.

En otras palabras, demostrar la validez del teorema matemático $A \to B$ equivale a demostrar la validez de su contrarrecíproco $\neg B \to \neg A$.

Ejemplo 241

De ser un número entero múltiplo de 10, ¿es posible deducir que es múltiplo de 5?

Resolución.— Esto es, ¿$(\forall x \in \mathbb{Z})(x$ múltiplo de 10 $\to x$ múltiplo de 5$)$? Pues sí. En efecto, usando la ley de contraposición, la pregunta es equivalente a: ¿$(\forall x \in \mathbb{Z})$(si x no es múltiplo de 5, entonces no es múltiplo de 10)? Y esto es cierto, pues estando A y B definidos como anteriormente, $\neg B \equiv (\forall n \in \mathbb{Z})(x \neq n{\cdot}5)$; en particular, sea un entero de la forma $n = k{\cdot}2$, entonces: $(\forall k \in \mathbb{Z})(x \neq k{\cdot}2{\cdot}5)$, lo que equivale a $(\forall k \in \mathbb{Z})(x \neq k{\cdot}10)$ y esto último a $\neg A$. ■

[11] *Cfr. supra* observación 2.2.10 (pág. 199 de esta edición).

§ 7.13.3 La estrategia de la reducción al absurdo

También conocida como *la estrategia de la contradicción*. Esta estrategia corresponde a la regla de reducción al absurdo (Abs, RAA)[12], esto es, $A \dashv\vdash (\neg A \vdash \bot)$.

En otras palabras, demostrar la validez del teorema matemático $A \to B$ equivale a demostrar la validez de su forma absurda $(A \wedge \neg B) \to \bot$.

Ejemplo 242

De ser un número entero múltiplo de 10, ¿es posible deducir que es múltiplo de 5?

Resolución.— Esto es, ¿$(\forall x \in \mathbb{Z})(x$ múltiplo de $10 \to x$ múltiplo de 5)? Pues sí. En efecto, usemos reducción al absurdo (Abs, RAA). Designemos x es múltiplo de 10 por A y x es mútiplo de 5 por B. Supongamos ahora que ocurriese $A \wedge \neg B$, esto es, x es múltiplo de 10 y x no es mútiplo de 5, pero esto conduce a contradicción, pues si x es múltiplo de 10, entonces x es de la forma $5k$, para algún k entero, de donde x es múltiplo de 5; la contradicción consiste en que se tiene a la vez que x es múltiplo de 5 (resultado de ser múltiplo de 10) y que x no es múltiplo de 5 ($\neg B$). Por lo tanto, por reducción al absurdo, tenemos que $A \to B$, justo lo que queríamos demostrar. ■

Ejemplo 243

$(\forall z \in \mathbb{Z})$ (z^2 es par $\to z$ es par).

Resolución.— En efecto, si z^2 es par, no puede ser z impar, porque si lo fuese, entonces $(\exists k \in \mathbb{Z})(z = 2k+1)$, de donde $(\exists k \in \mathbb{Z})(z^2 = (2k+1)^2 = 4k^2 + 1^2 + 4k = 2(2k^2+2k)+1)$, esto es, $(\exists k' \in \mathbb{Z})(z^2 = 2k'+1)$, es decir, z^2 es impar; he aquí una contradicción, z^2 es a la vez impar y par; por lo tanto, por reducción al absurdo tenemos justo lo que queríamos demostrar. ■

Ejemplo 244

¿Si un número real sumado consigo mismo es él mismo, entonces tal número es el cero?

Resolución.— Sí. En efecto, sea $x \in \mathbb{R}$, $A \wedge \neg B \leftrightarrow x + x = x \wedge x \neq 0$; al ser $x \neq 0$, es admisible dividir $2x = x$ entre x, lo cual conduce a la fórmula insatisfactible $2 = 1$. Por lo tanto, por reducción al absurdo, $x = 0$. ■

[12] *Cfr. supra* teorema 2.35 (pág. 214 de esta edición) y observación 2.2.36 (pág. 214 de esta edición).

Ejemplo 245

Demostremos que si r^* es un racional no nulo e i es un irracional, entonces el producto $r^* \cdot i$ es irracional.

Resolución.— Usemos para ello reducción al absurdo; si no fuese irracional, sería racional, esto es, existirían $p \in \mathbb{Z}$, $q \in \mathbb{Z}^+$, tales que $r^* \cdot i = p/q$, de donde, $i = \dfrac{p}{r^* \cdot q}$, esto es, i sería racional (por serlo el producto y división de racionales); he aquí una contradicción, i sería a la vez irracional y racional; por lo tanto, queda demostrado por reducción al absurdo lo que afirma el enunciado. ■

Ejemplo 246

Demostremos que $\log_{10} 2$ es irracional.

Resolución.— Sea $r = \log_{10} 2$; por definición de logaritmo, $10^r = 2$ (las funciones $\log_b x$ y b^x son inversas siendo $b \in (1, \to)$ y $x \in (0, \to)$); razonemos por reducción al absurdo; si r no fuese irracional, sería racional, esto es, existirían $p \in \mathbb{Z}$, $q \in \mathbb{Z}^+$, tales que $r = p/q$; sustituyendo en la ecuación anterior, $10^{p/q} = 2$, de donde, elevando ambos miembros a la potencia q, $\left(10^{p/q}\right)^q = 2^q$, esto es, $10^p = 2^q$, y de aquí, factorizando, $2^p 5^p = 2^q$; como p y q son enteros y 2 y 5 son primos, estamos ante una igualdad de dos descomposiciones en factores primos, por lo que los exponentes de éstos deben ser iguales, esto es, de los exponentes de 2, $p = q$, y de los exponentes de 5, $p = 0$; por lo tanto, $p = 0$ y $q = 0$; he aquí una contradicción, $q = 0$ y $q \neq 0$ (es el denominador de una fracción); por lo tanto, por reducción al absurdo tenemos que $\log_{10} 2$ es irracional. ■

Ejemplo 247

Si dos móviles infinitesimales parten del punto medio de la base de un triángulo equilátero con la misma velocidad constante, recorriendo uno la altura (ida y vuelta, otra vez ida y vuelta, y así sucesivamente, sin parar) y el otro el perímetro (una y otra vez, y así sucesivamente, sin parar), ¿coincidirán alguna vez?

Resolución.— Sea A el móvil que recorre la altura y B el que recorre el perímetro; sea h la altura y $2l$ la longitud de un lado, entonces, por el teorema de Pitágoras, $h^2 = (2l)^2 - l^2 = 3l^2$, esto es, la altura mide $h = l\sqrt{3}$; razonemos por reducción al absurdo: si se encontrasen de nuevo, A habría recorrido un número de veces, digamos m $(\in \mathbb{Z}^+)$, la altura, y B, un número de veces, digamos n $(\in \mathbb{Z}^+)$, la mitad del lado, en otras palabras, $mh = nl$, de donde, $ml\sqrt{3} = nl$, por lo que $m\sqrt{3} = n$, lo cual es una contradicción pues según esto el producto $m\sqrt{3}$ es racional, pero como $\sqrt{3}$ es irracional, sabemos (Cubit 3) que dicho producto es irracional; por lo tanto, por reducción al absurdo deducimos que los móviles no coincidirán. ■

Observación 7.13.0.— Alternativamente, de $m\sqrt{3} = n$ se sigue $\sqrt{3} = n/m$, esto es, que $\sqrt{3}$ es racional; he aquí una contradicción, pues sabemos que $\sqrt{3}$ es irracional; por lo tanto, por reducción al absurdo deducimos que los móviles no coincidirán.

Ejemplo 248

Un plano ha sido pintado arbitrariamente usando dos colores (un ejemplo es un mantel blanco sobre el que se ha derramado tinta). Demostremos que siempre es posible hallar un segmento de longitud uno cuyos extremos son de un mismo color.

[Cubit 17], *Vid.* Zhúkov, Samovol y Applebaum [86]: problema 3 (pág. 28).

Resolución.— La cuestión se plantea en un plano y con él debemos razonar (el mantel, un paralelogramo, es sólo una metáfora aclaratoria). Por otra parte, para afirmar que encontrar un segmento de extremos de distinto color es una contradicción, debemos haber admitido en algún momento que todos los segmentos que pudiésemos encontrar tienen sus extremos de un mismo color, pero ésto implica haber incluido como hipótesis lo que queremos demostrar, a saber, que es posible encontrar un segmento con sus extremos de un mismo color.

Queremos demostrar una afirmación con la estructura $P \rightarrow Q$, representando P el hecho de tener un plano coloreado con dos colores y Q que es posible encontrar un segmento de longitud 1 cuyos extremos sean de un mismo color. Para razonar por reducción al absurdo (Abs, RAA), debemos suponer $P \wedge \neg Q$, esto es, que tenemos el plano coloreado con dos colores (P) y que no es posible encontrar un segmento de longitud 1 cuyos extremos sean de un mismo color ($\neg Q$) (en otras palabras, que en dicho plano, todos los segmentos de longitud 1 tienen sus extremos de colores distintos). Ahora se trata de demostrar que de ello se deriva una contradicción, para, finalmente, aplicar RAA y deducir que, en efecto, se tiene $P \rightarrow Q$.

Hagámoslo. Supongamos que tenemos el plano coloreado con dos colores (P) y que no es posible encontrar un segmento de longitud 1 cuyos extremos sean del mismo color ($\neg Q$). En dicho plano, pensemos ahora en un triángulo equilátero ABC de lado 1. Debido a suponer $\neg Q$, A y B deben ser de distinto color y también deben serlo A y C, esto es, hablamos de tres colores distintos (ya que B y C también son extremos de un segmento de longitud 1). Hemos llegado a una contradicción, a saber, el plano está coloreado con dos colores (P) y a la vez lo está con tres (hemos deducido esto último). Así nuestra suposición era falsa. Por tanto, por reducción al absurdo, deducimos la veracidad de lo afirmado en el enunciado de la cuestión. ■

Observación 7.13.1.— El ejemplo anterior es un clásico que también aparece con relativa frecuencia en libros sobre combinatoria, en relación con la teoría de Ramsey euclidea. Además, tiene que ver con el Problema de Hardwiger y Nelson[13], aún no resuelto, en teoría de grafos.

[13] *Vid. v. gr.* https://en.wikipedia.org/wiki/Hadwiger%E2%80%93Nelson_problem.

Ejemplo 249

Existen múltiples variantes del juego del ajedrez. En una de ellas con jugada doble, las reglas del juego son las mismas que en el ajedrez, con la excepción de que quienes juegan pueden hacer a voluntad una o dos jugadas seguidas. Demostremos por reducción al absurdo que quien inicia el juego tiene una estrategia que le garantiza al menos las tablas.

Vid. ZHÚKOV, SAMOVOL y APPLEBAUM [86]: problema 2 (pág. 28).

Resolución.— Supongamos lo contrario, esto es, que quien inicia el juego, pierde. Digamos que comienzan blancas. Pero como es de jugada doble, en la jugada inicial esta persona puede recrear la posición original del tablero —bastaría, por ejemplo, que moviese un caballo a una posición accesible y la devolviese a su posición original—. Así, el papel de persona que inicia el juego ahora es de quien juega negras. Pero como inicia el juego, pierde. Total, que ambas personas pierden. Lo cual no es posible, es una contradicción. Por reducción al absurdo, se sigue lo contrario al punto de partida, quien inicia no pierde, esto es, que como mínimo consigue tablas.[14] ■

Ejemplo 250

Dado que en un triángulo el lado mayor y el ángulo mayor son opuestos, pudiese conjeturarse que, en general, en un triángulo, las longitudes de los lados son proporcionales a las magnitudes de sus ángulos opuestos. Ahora bien, si esto fuese verdad, en un triángulo de ángulos 30, 60 y 90 grados, los lados serían proporcionales a 1, 2 y 3, esto es, que sus lados x, y, z, seguirían la proporción $x : y : z = 30 : 60 : 90 = 1 : 2 : 3$. Pero esto no es cierto, ¿verdad?

[Cubit 18]. *Cfr.* ZHÚKOV, SAMOVOL y APPLEBAUM [86]: pág. 29.

Resolución.— Veamos. Supongamos que siguen dicha proporción; los lados son $x = k$, $y = 2k$, $z = 3k$, un ángulo es de 90 grados, el lado mayor es $z = 3k$ que es la hipotenusa, los otros lados son $x = k$ e $y = 2k$; por el teorema de Pitágoras, $(3k)^2 = k^2 + (2k)^2$, esto es, $9k^2 = k^2 + 4k^2$, o sea, $9k^2 = 5k^2$, de donde, por ser $k > 0$, deducimos que $9 = 5$, es decir, una contradicción; de

[14] No me resisto a citar aquí la resolución aportada por Alejandro FERNÁNDEZ CAMELLO (año académico 2019-2020), por si es más clarificadora: «Partimos de que en una partida de ajedrez hay únicamente tres resultados posibles desde la perspectiva de las blancas ganan, empatan o pierden. Queremos demostrar que existe una estrategia para las blancas de al menos poder empatar, suponemos que la negación de esta hipótesis es verdadera, es decir, que las negras poseen una estrategia ganadora para cualquier estrategia del blanco. Las blancas pueden hacer dos jugadas en su turno, y tienen cuatro maneras (Cf3 Cg1,Ch3 Cg1, Cc3 Cb1, Ca3 Cb1) de mantener la posición inicial cediéndole el turno a las negras, es decir, que las blancas pasarían a ser las negras y viceversa. Por tanto, las blancas contarían también con una estrategia ganadora para cualquier estrategia negra llevándonos a una contradicción y al aplicar reducción al absurdo obtenemos que nuestra hipótesis inicial de que las blancas tienen al menos una estrategia para empatar resulta verdadera».

aquí, por reducción al absurdo, deducimos que no siguen dicha proporción. Por lo tanto, no es cierto que en todo triángulo, las longitudes de los lados son proporcionales a las magnitudes de sus ángulos opuestos. ■

Ejemplo 251

Si x es una palabra de $\{0,1\}^*$, entonces $0x \neq x1$.

[Cubit 20].

Resolución.— Consideremos una palabra x con $|x| = n$;[15] por un lado, $(0x)_1 = 0$ y $(0x)_{i+1} = x_i$, y $(x1)_{n+1} = 1$ y $(x1)_i = x_i$; por otro, supongamos que $0x = x1$, como dos palabras son idénticas si lo son letra a letra, entonces $0 = (0x)_1 = (x1)_1 = x_1$, $x_1 = (0x)_2 = (x1)_2 = x_2$, $x_2 = (0x)_3 = (x1)_3 = x_3$, $\ldots$, $x_{n-1} = (0x)_n = (x1)_n = x_n$ y $x_n = (0x)_{n+1} = (x1)_{n+1} = 1$, esto es, $0 = x_1 = x_2 = x_3 = \cdots = x_{n-1} = x_n = 1$, es decir, $0 = 1$, o sea, una contradicción; de aquí, por reducción al absurdo, deducimos que $0x \neq x1$.[16] ■

§ 7.13.4 La estrategia del dilema

Esta estrategia corresponde a la regla de inferencia deductiva *dilema constructivo simple* (DCS), esto es, $A \vee B, A \rightarrow C, B \rightarrow C \vdash C$. Por tanto, lo que nos preocupa es demostrar $A \rightarrow C$ y $B \rightarrow C$ para después inferir C de $A \vee B$ vía DCS.

§ 7.13.5 La estrategia de la prueba por casos

También llamada *la estrategia de la exhaustividad*. Apropiada cuando tenemos un *universo finito*. A veces, este tipo de demostración aparece con el nombre de *inducción perfecta* o *exhaución*.

Se basa en la regla deductiva de eliminación del disyuntor (ED), también conocida por regla o prueba por casos (Cas), esto es, $A \vee B, A \vdash C, B \vdash C \vdash C$; es decir, lo que nos preocupa es demostrar que C se deduce de A y que C también se deduce de B para después inferir C de $A \vee B$ vía Cas.

Ejemplo 252

Demostremos que todos los números impares mayores que 0 y menores que 9 son primos.

Resolución.— En este caso, basta que analicemos uno a uno los números 1, 3, 5 y 7, que resultan ser todos primos y por tanto, verdadero lo postulado. ■

[15] Libres somos de acudir a una interpretación más allá de la alfabética, por ejemplo, al ser un alfabeto de sólo dos letras, como una tupla de n valores de verdad de ciertas proposiciones x_i.

[16] *Vid. infra* una demostración por inducción fuerte en el ejemplo 418 (p. 812).

Ejemplo 253

En el sistema decimal, hallemos todos los números primos de dos cifras, xy e yx (permutado del anterior), tales que su suma es un número capicúa.

Resolución.— Como hemos discutido en el ejemplo ejemplo 233 (pág. 467 de esta edición), sólo hemos de analizar los primos 11, 13, 17, 19, 37 y 79.

Veamos, pues:

$11 + 11 = 22$, sí;
$13 + 31 = 44$, sí;
$17 + 71 = 88$, sí;
$19 + 91 = 110$, no, pues 91 no es primo;
$37 + 73 = 110$, no, pues 110 no es capicúa;
$79 + 97 = 176$, no, pues 176 no es capicúa. 

§ 7.14 La estrategia de la inducción

La estudiaremos en § 16 (pág. 804 de esta edición). Veremos *inducción débil*, *inducción fuerte* e *inducción estructural*. Nos referimos a ellas aquí en aras de la compilación y la unidad.

§ 7.15 La estrategia combinatoria

En parte la estudiaremos en § 19 (pág. 1124 de esta edición), en parte aquí.

Muchas personas argumentan que una demostración algebraica es directa. Sin embargo, muchas demostraciones algebraicas son instrumentales, sistemáticas y, precisamente por eso, automáticas y automatizables.

La demostración combinatoria tiene un punto de ingenio, belleza y arte e incluso de diversión, difícilmente inigualable por una demostración algebraica.

Ejemplo 254

Proporcionemos una demostración algebraica y una demostración combinatoria de la simetría de la elección: si $0 \leq k \leq n$, entonces $C(n, k) = C(n, n - k)$.

Resolución.— La siguiente es un ejemplo de *demostración algebraica* que es, simplemente, aburrida.

$C(n,k) = n!/(k! \cdot (n-k)!)$ [definición de combinación] $= n!/((n-k)! \cdot k!)$ [conmutatividad de la multiplicación entera] $= n!/((n-k)! \cdot (n-(n-k))!)$ [antisimplificación: $k = n-(n-k)$] $= C(n, n-k)$ [definición de combinación].

A continuación, un ejemplo de *demostración combinatoria*, sin duda, creativa.

Una palabra de n bits con k unos es una palabra de n bits con $n-k$ ceros [«es», esa es la clave], por lo tanto el número de palabras de n bits con exactamente k unos es el mismo que el número de palabras de n bits con exactamente $n-k$ ceros. ■

Aquí, además, destacamos las siguientes.

§ 7.15.0 Las estrategias de los principios fundamentales de recuento

Estudiadas en § 19.1 (pág. 1136 de esta edición), son las estrategias correspondientes a: el *principio de la adición*, el *principio de la multiplicación*, el *principio del complementario*, el *principio de la división*, el *principio restringido de los cajones de* Dirichlet, el *principio generalizado de los cajones de* Dirichlet y el *principio de inclusión-exclusión*.

Nos referimos a ellas aquí en aras de la compilación y la unidad.

§ 7.15.1 La estrategia de la paridad

En esta estrategia media una entidad que tenga asociados dos estados posibles —y que en ausencia de perturbaciones pueda permanecer indefinidamente en uno de ellos— y contar el número de cambios de estado, para, finalmente conseguir la demostración de la cuestión que se está tratando teniendo en cuenta que si el número de cambios de estado es par, la entidad tiene asociado el estado que tenía antes de comenzar los cambios de estado, pero si dicho número es impar, la entidad tiene asociado el otro estado.

Ejemplo 255

Ver la moneda apoyada en la palma de la mano y contar el número de vueltas que da una moneda en el aire, ¿sirve para saber qué cara muestra al final?

Resolución.— Sí, si da un número par de vueltas, mostrará la misma cara que al principio; sin embargo, si da un número impar de vueltas, mostrará la otra cara. ■

§ 7.15.2 La estrategia de la biyección

Conocida también como el *principio de correspondencia*, consiste en encontrar una biyección entre dos conjuntos para así demostrar que ambos tienen el mismo cardinal.

§ 7.15.3 La estrategia de la doble cuenta

En esta estrategia media encontrar un conjunto y contar de dos maneras distintas el número de sus elementos, para, finalmente, vía la igualación de los resultados obtenidos conseguir la demostración de la cuestión de que se está tratando.

Ejemplo 256

Demostremos que $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Resolución.— Para ello, nos preguntamos de cuántas formas pueden disponerse en hilera (alinearse) los primeros n números enteros positivos y responderemos contando de dos maneras diferentes dichas disposiciones (alineaciones).

Primera cuenta.— Cada disposición es una permutación de n elementos, por lo que el número de disposiciones es el número de permutaciones de n elementos, esto es, $n!$.

Segunda cuenta.— Aplicaremos el principio de la multiplicación[17]. Sea $S \leftrightharpoons$ disposición en hilera de los primeros n números enteros positivos. La realización de S sucede en tres fases consecutivamente independientes: $S_0 \leftrightharpoons$ elección de k elementos de los n; $S_1 \leftrightharpoons$ disposición en hilera de tales k elementos; $S_2 \leftrightharpoons$ disposición en hilera de los $n-k$ elementos restantes. Estas tres fases pueden realizarse: S_0, de $\binom{n}{k}$ formas; S_1, de $k!$ formas, y S_2, de $(n-k)!$ formas. Por el principio de la multiplicación, $\#S = \#S_0 \cdot \#S_1 \cdot \#S_2 = \binom{n}{k} \cdot k! \cdot (n-k)!$.

De igualar ambas cuentas:

$$n! = \binom{n}{k} \cdot k! \cdot (n-k)!,$$

de donde:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}.$$

■

§ 7.15.4 La estrategia del elemento distinguido

Sea un conjunto C y destaquemos un elemento suyo, digamos, x; a este elemento que destacamos es al que denominamos elemento distinguido. Sea $P(X, x)$ un predicado diádico, donde $X \subseteq C$. Sean S una colección de subconjuntos de C, S^+ la colección de subconjuntos X de C en S que satisfacen $P(X, x)$ y S^- la colección de subconjuntos X de C en S que no satisfacen $P(X, x)$. Por esta definición, $S^+ \cap S^- = \emptyset$, de donde por el principio de la adición[18], $|S| = |S^+| + |S^-|$, con lo que

[17] *Vid. infra* § 19.1.1 (pág. 1138 de esta edición).
[18] *Vid. infra* § 19.1.0 (pág. 1136 de esta edición).

la colección S de subconjuntos de C ha quedado particionada en dos subcolecciones disjuntas, S^+ y S^-, de acuerdo a un elemento distinguido x de C y un predicado.

Ejemplo 257

Sirva como tal el ejemplo 411 (pág. 806 de esta edición).

Resolución.— En efecto, allí: C es X; S es 2^X; $P(X, x) \leftrightharpoons x \in X$; S^+ es la colección de subconjuntos de X en S tales que $x \in X$; S^- es la colección de subconjuntos de X en S tales que $x \notin X$; $|S^+| = 2^k$, y $|S^-| = 2^k$. ■

§ 7.16 La estrategia de la probabilidad

Si bien no trataremos de ella explícitamente en estas notas, sí que lo haremos implícitamente cuando estudiemos combinatoria[19], al trabajar con operaciones de recuento. Además, nos sumergiremos brevemente en un impromptu probabilístico[20] y propondremos un impromptu estadístico[21]. En todo caso, nos referimos a ella aquí en aras de la compilación y la unidad.

Un ejemplo relevante es el problema de Monty Hall[22].

§ 7.17 Un ejemplo recapitulatorio, en parte, sólo en parte

Ejemplo 258

La suma de dos números enteros consecutivos es impar.

Resolución.— Reescrita en forma más próxima al lenguaje proposicional, tenemos:

si dos números son consecutivos, *entonces* su suma es impar.

Para cualesquiera dos números m, n, si n es el siguiente a m, entonces, $n + m$ es impar.

Como hablamos de números consecutivos, es admisible pensar en $\mathbb{N}$ o $\mathbb{Z}$, con el orden habitual (incluso pudiésemos pensar en cualquier conjunto numerable[23] con el orden inducido por la biyección con $\mathbb{N}$).

[19] *Cfr. infra* § 19 (pág. 1124 de esta edición).
[20] *Cfr. infra* § 19.9 (pág. 1286 de esta edición).
[21] *Cfr. infra* actividad A.3 (pág. 1428 de esta edición).
[22] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Monty_Hall_problem.
[23] *Cfr. infra* § 13.4 (pág. 729 de esta edición).

- Vamos a demostrarlo para los naturales, *sin pérdida de generalidad* (esto quiere decir que una demostración para los enteros sería análoga). En definitiva, queremos demostrar que

$$(\forall m, n \in \mathbb{N})(n = m + 1 \rightarrow n + m \text{ es impar}).$$

- $0 + 1 = 1, 1 + 2 = 3, 2 + 3 = 5, 3 + 4 = 7$; si nuestro interés hubiese sido demostrar que algún par de números consecutivos suma impar, ya lo habríamos demostrado, pues hemos encontrado cuatro ejemplos (en realidad, hubiese bastado con uno) —habríamos hecho una *demostración con ejemplos*—;

- A estas alturas pudiésemos incluso atrevernos a *conjeturar* que la suma no sólo es un número impar, sino que es un número primo (salvo la primera que ha sido 1) —las primeras sumas han sido 1, 3, 5 y 7—. Sin embargo, con la suma siguiente comprobamos que no es así, $4 + 5 = 9$ —acabamos de hacer una *demostración por contraejemplos* de la falsedad de la afirmación de que la suma de dos números consecutivos es un número primo—.

- Bueno, veamos que sí es cierta la afirmación original: $a+(a+1) = 2a+1$ es impar por definición de número impar. Esto ha sido una *demostración directa*.

- Razonemos ahora «al revés». Supongamos que no fuese impar la suma, entonces es que es par, esto es, que $2a + 1$ es par, o sea, que $2a + 1$ es de la forma $2k$; pero entonces pudiésemos pensar en demostrar directamente que no puede descomponerse en dos sumandos que sean números consecutivos. Esto no es difícil.

$$\begin{aligned} a + b &= 2k \\ a - k &= b - k \\ -(k - a) &= k - b \\ |k - a| &= |k - b|, \end{aligned}$$

  esto es, k está a la misma distancia de a que de b, y esto entre números, significa que k está entre a y b, con lo que, o los tres son iguales o los tres distintos, en cualquier caso, a y b no son consecutivos. Acabamos de hacer una *demostración por contraposición*.

- Claro que una vez que tenemos que $2a + 1$ es de la forma $2k$, pudiésemos pensar que entonces, $1 = 2(k - a)$, es decir, 1 es el doble de un número entero ($k - a$ es entero por serlo k y a), en otras palabras, que 1 es par, y he aquí que hemos obtenido una contradicción, que 1 no es par (esto lo sabíamos) y que a la vez 1 es par, algo imposible —lo que acabamos de hacer ha sido una *demostración por reducción al absurdo*: queríamos demostrar $P \rightarrow Q$, para lo que hemos supuesto que no es cierto, esto es, que lo que sucede es $\neg(P \rightarrow Q)$, o sea, $P \wedge \neg Q$, es decir, que mientras que P sí es cierto (la suma lo es de dos números consecutivos), Q no lo es (no es cierto que la suma sea impar), y hemos obtenido una contradicción, de donde deducimos que no puede suceder $P \wedge \neg Q$ (pues nos conduce a una contradicción) sino que lo que es cierto es $P \rightarrow Q$.

- También pudiésemos pensar en una *demostración por casos*. Pensemos en partir los naturales en dos subconjuntos disjuntos, el de los pares y el de los impares y considerar dos casos cuya disyunción conforma el total, A) que la primera componente de la pareja de números consecutivos sea para o bien B) que sea impar. Si es par, entonces la suma es, digamos, $2k + (2k + 1)$, con $k \in \mathbb{N}$, esto es, $4k + 1$, en otras palabras, impar; por otro lado, si es impar, entonces la suma es, digamos, $(2k - 1) + 2k$, con $k \in \mathbb{Z}^+$, esto es, $4k - 1$, es decir, también impar.

- Finalmente también pudiésemos haber hecho una *demostración por reducción* de nuestro problema a uno más general, en este caso de que la suma de un número par $2k$ y un impar $(2h + 1)$ es impar, ya que por la distributiva del producto respecto de la suma, $2k + (2h + 1) = 2(k + h) + 1$ que es impar por definición de impar, ya que al ser k y h enteros, también lo es $k + h$. ■

§ 7.18 Matemática y computación: la estrategia algorítmica

«La matemática es la ciencia más barata. A diferencia de la física o la química, no requiere equipos costosos. Todo lo que se necesita para hacer matemáticas es lápiz y papel» (George Pólya).

Al principio eran cuatro: uno en Filadelfia, otro en Aberdeen, otro en Cambridge y otro en Washington. Pronto fueron diez. De repente, doscientos. La última cifra que se manejó fue de 35000; después, se perdió la cuenta. Los computadores proliferaron, generación tras generación; en los 80, una calculadora de bolsillo, que costaba unas pocas miles de pesetas, tenía ya mayor capacidad de cómputo que aquellas mastodónticas moles: los ENIAC, MARK, SEAC y GOLEM. En la actualidad, los móviles, diríamos que ya a «años luz» de aquéllos, han invadido los comercios y a punto están de convertirse en un objeto de usar y tirar —ojalá no, por el bien del medioambiente—, como las hojas de afeitar o los pañuelos de papel.

Cuenta la leyenda que, cuando a finales del decenio de los cuarenta del siglo XX, Thomas John Watson, de IBM, supo de las potencialidades del computador digital, estimó que, como mucho, tres bastarían para cubrir las necesidades de cómputo de todos los Estados Unidos. Nadie pudo prever, por aquél entonces, hasta qué punto se incrementarían tales necesidades, hasta agotar por completo toda la capacidad de cómputo disponible.

La relación entre la matemática y la ciencia e ingeniería de la computación ha sido mucho más compleja de lo que desde la profanidad pudiese sospecharse. Casi todo el mundo supone que quien se declare profesional de la matemática ha de utilizar computadores. La realidad es que, contrariamente a lo que ocurre en otras ramas de las humanidades y la ciencia, la mente matemática se ha mostrado indiferente al computador, ignorando incluso cómo utilizarlo —reduciendo, a veces, su utilización a la de una muy potente máquina de escribir electrónica con un amplio procesamiento de textos y fuentes matemáticas—. Aún más, la idea misma de que el trabajo de creación matemática pudiese quedar mecanizado les parece a muchas de estas mentes que va en menoscabo de su estimación profesional. Evidentemente, quienes trabajan en matemática aplicada, estadística o investigación operativa, codo

a codo con otras ramas de la ciencia e ingeniería, con el propósito de obtener soluciones numéricas de problemas prácticos, han encontrado en el computador un auxiliar indispensable.

Son muy numerosos los teoremas que afirman la existencia de determinados objetos matemáticos, pero no todas las demostraciones conllevan la construcción efectiva de tales objetos. No fue así siempre; las primeras matemáticas, egipcia, babilónica y del antiguo Oriente, fueron todas ellas *algorítmicas*, en el sentido de que describían construcciones (algoritmos) para generar resultados. La matemática *dialéctica* —estrictamente lógica, deductiva— se originó en la Grecia clásica, aunque no desplazó a la algorítmica: recordemos a EUCLIDES, para quien el papel de la dialéctica es la justificación de un algoritmo.

Es sólo en tiempos modernos cuando encontramos matemáticas de escaso o nulo contenido algorítmico, a las que pudiésemos calificar de puramente dialécticas o existenciales.

Una de las primeras investigaciones que dio claras muestras de espíritu e inspiración predominantemente dialéctica es la búsqueda de las raíces de los polinomios de grado n. Al no poderse encontrar una fórmula explícita que permitiese calcularlas en función de los coeficientes, la cuestión pasó a ser aproximar esas raíces y, en última instancia, garantizar la existencia de las mismas. Los teoremas que así lo garantizan (de GAUSS, de GALOIS) son teoremas dialécticos. El aspecto algorítmico sigue siendo actualmente objeto de análisis.

Durante la mayor parte del siglo XX, la matemática ha sido más existencial que algorítmica. En la última década del XX y en las primeras del XXI, no obstante, apreciamos un desplazamiento hacia la algoritmia. Pudiese deberse esto a la llegada de una generación de profesionales de la matemática que aprendieron a programar computadores ya en los últimos cursos de enseñanza media (y en breve, con las tantas reformas educativas de la modernidad, incluso desde antes de la primaria). Comenzamos a detectar un cambio en la investigación matemática; existe un interés más acentuado por los resultados de carácter constructivo o algorítmico, y menor en cambio, por los de naturaleza puramente existencial o dialéctica, casi carentes de significado computacional (no del todo, pues son básicos, por poner un ejemplo, en el desarrollo de un motor de inferencia para un sistema de producción basado en reglas —sistema experto—). Así, la matemática se ve afectada por la disponibilidad de computadores, que incita a quienes investigan en ella hacia campos en los que el computador puede desempeñar algún papel. A pesar de lo dicho, incluso en nuestros días, es cierto que una amplísima parte de la investigación matemática se desarrolla sin utilizar los computadores, ni actual ni potencialmente. Curiosamente, donde sí sucede, esencialmente por la ingente cantidad de datos que hay que manejar, han aparecido nombres nuevos para ramas consolidadas de la matemática: por ejemplo, minería, análisis y ciencia de datos para subespecializaciones consagradas de la Estadística y la Investigación Operativa.[24]

[24] Este fenómeno de renombramiento se ha propagado con facilidad por la sociedad, afectando a materias y campos de conocimiento diversos, por ejemplo, en la literatura, a obras de Agatha CHRISTIE y Roald DAHL. Tanta ideología y postmodernismo. Pura censura. Tanto desprecio a la historia. Puro denuesto. Se intuía que llegaríamos a este estado de cosas. Pues, hala, a reescribir el pasado a nuestro gusto. ¡Cómo me recuerda *Fahrenheit 451* de BRADBURY! Por el bien de la humanidad esperemos que como allí quede copia del original a buen recaudo.

En matemática aplicada, el computador sirve para calcular soluciones aproximadas cuando la teoría no es capaz de darnos una solución exacta. Es aceptable tratar de utilizar nuestra teoría para demostrar que la solución computada se aproxima, en cierto sentido, a la solución exacta. Pero la teoría no depende para nada del computador para obtener sus conclusiones; más bien, ambos métodos, el teórico y el mecánico, son como dos puntos de vista independientes de y para la misma cuestión a resolver. El asunto es coordinarlos.

En teoría de números, en problemas como *la distribución de los números primos*, el computador sirve para generar datos. Estudiando estos datos, las mentes educadas matemáticamente pueden lograr formular una conjetura. Evidentemente, les gustaría demostrar la conjetura formulada; en caso de no conseguirlo, podrían «ponerla a prueba» volviendo a utilizar el computador para examinar otra muestra y ver si el resultado predicho por su conjetura se confirma.

En ambos casos, la matemática rigurosa de la demostración permanece inviolada por el computador. En matemática aplicada, éste permanece en segundo lugar, como instrumento o sucedáneo a utilizar allí donde la teoría no es capaz de trabajar. En teoría de números, el computador «asesora» heurísticamente, lo cual puede ayudarnos a decidir qué creer, e incluso el grado de creencia que debemos asumir. Pero sigue sin afectar a lo que se demuestra.

Citemos un problema en el que los computadores han intervenido en la demostración: *la conjetura de los cuatro colores*. Este problema consiste en demostrar que todo mapa trazado sobre una superficie plana o sobre una esférica, puede ser coloreado sin utilizar más de cuatro colores distintos (tetracromático), de forma que todas las regiones sean conexas y que dos regiones adyacentes cualesquiera no sean del mismo color.

En este sentido hablamos de una nueva estrategia de demostración, que comúnmente es referida como *demostración asistida por computador*.

Pues bien, este problema fue planteado en 1852 por Francis GUTHRIE; en 1878, Arthur CAYLEY lo volvió a plantear a la *London Mathematical Society*, y antes de un año, Alfred Bray KEMPE, miembro de esta sociedad, había publicado un artículo donde afirmaba haberlo demostrado. Su razonamiento consistió en una reducción al absurdo. Como a todo mapa puede asociársele un mapa normal (nunca se encuentran en un mismo punto más de tres regiones y ninguna de las regiones envuelve completamente a las demás), basta demostrarla para éstos. KEMPE demostró, correctamente, que en todo mapa normal hay al menos una región que tiene como máximo cinco vecinas; esto genera un conjunto de cuatro configuraciones «inevitables». A continuación, trató de mostrar de qué forma pudiese construirse en todo caso de mapa forzosamente pentacromático un mapa de menor número de países que siguiera siendo pentacromático. Cuando esto se puede llevar a cabo, decimos que la configuración es «reducible». Así pues, la idea de KEMPE consiste en exhibir un conjunto inevitable de configuraciones reducibles. Si puede hacerse, pudiésemos concluir que dado un mapa pentacromático cualquiera, a partir de él se podría construir un mapa pentacromático con menor número de

regiones, y en un número finito de pasos llegaríamos a tener un mapa pentacromático con menos de cinco regiones, lo cual es absurdo.

Mas en 1890, Percy John HEAWOOD, descubre un error en el razonamiento de KEMPE sobre reducibilidad en el caso de una región con cinco vecinas. Desde 1890 hasta 1976 permaneció abierta la conjetura.

En 1976, Kenneth Ira APPEL y Wolfgang HAKEN anuncian haberla demostrado con ayuda de un computador. La idea de la demostración sigue siendo la misma, sólo que el conjunto inevitable, en vez de las cuatro de KEMPE, contiene 1936 configuraciones distintas, la mayor parte de una complicación tal, que la única forma de poder demostrar su reducibilidad tuvo que ser con ayuda de un computador de alta velocidad (a pesar de lo cual necesitaron 1200 horas de cálculo).

Debemos mencionar que más tarde, Daniel COHEN llevaría el estudio de este problema al estudio de trece matrices particulares, lo que le confiere «una talla más humana».

Los servicios prestados por el computador en este caso fueron, en principio, de naturaleza muy distinta a los que hemos descrito en los casos de la matemática aplicada y la teoría de números. APPEL y HAKEN presentan su trabajo como «una demostración completa, definitiva y rigurosa». Ellos mismos sugieren que su demostración «sugiere que existe un límite para lo conseguible por métodos puramente teóricos, incluso dentro de las Matemáticas [sic]. De ella se deduce también que en el pasado se ha subestimado la necesidad de métodos computacionales en las demostraciones matemáticas».

Filósofos como Thomas TYMOCZKO [120], objetan que desde el punto de vista filosófico, utilizar el computador como parte esencial de la demostración comporta un debilitamiento de las normas de la demostración matemática. Proporciona bases al escepticismo, y con ello altera de modo fundamental la situación, en la que antes se suponía que la demostración conducía a conclusiones indubitables, que no daban pie a escepticismo en ninguna de sus fases. La aceptación de tal demostración comporta un cierto acto de fe. Al descansar la misma en los resultados de un computador, está sacrificando una parte esencial de la certeza matemática, la está degradando al nivel vulgar del conocimiento ordinario, que está sujeto a un escepticismo posible y cierto del cual siempre estuvo libre el conocimiento matemático.

Sin embargo, a la mente matemática, la cuestión se le presenta bajo una luz enteramente diferente. Para la filosofía, existe una diferencia absoluta entre una demostración que depende de la fiabilidad de un computador y una demostración que sólo depende de la razón humana. Para la matemática, la fiabilidad de la razón es una de esas cosas de la vida, tan familiares, que puede dar al computador la bienvenida, teniéndolo como lo tiene por calculista más de fiar de lo que cualquier mente humana puede esperar llegar a ser sin ayuda artificial.

La probabilidad de error humano está presente incluso antes de hacer intervenir al computador. En la actualidad, aparentemente, lo más factible es intentar minimizarla. Pero si una demostración

es lo suficientemente larga y complicada (el teorema definitivo de clasificación de los grupos simples superará muy ampliamente las cinco mil páginas de revista —Daniel GORENSTEIN, *Bulletin of the American Mathematical Society*, enero de 1979—), siempre podremos albergar dudas acerca de su verdad. «El computador no elimina los errores humanos, pues él mismo es un producto humano» (DAVIS y HERSH [121]). Recordemos las palabras de Henry Peter Francis SWINNERTON-DYER citadas en esta obra: «la única forma de verificar estos resultados (si se considera que vale la pena) es volver a afrontar el problema de forma totalmente independiente, utilizando una máquina diferente. Proceder que se corresponde exactamente con el de la mayor parte de las ciencias experimentales».

La aparición de los computadores personales a finales de los setenta del siglo XX, revitalizó el cálculo numérico; antes de ello, hace sólo cincuenta años, era casi inexistente en algunos planes de estudio de las licenciaturas de matemática. También sirvió para despertar de un sueño cincuentenario a la teoría de matrices. Llamó la atención sobre la importancia de la lógica y de la teoría de las estructuras abstractas discretas; más generalmente, todo el conjunto de materias que se engloban en la matemática discreta, han ido encontrando aplicaciones en el ámbito computacional, lo que ha estimulado la investigación en estos campos. También provocó la creación de disciplinas nuevas, como la programación lineal, la geometría computacional o la teoría de complejidad computacional.

Por otro lado, el creciente desarrollo de la computación en los últimos años hace pensar en ella como una nueva ciencia y no como una mera colección de técnicas para resolver un determinado tipo de problemas. Esto se debe a que cada vez, con mayor frecuencia, se desarrollan principios generales y se fundamentan matemáticamente diversas áreas de la misma, como el análisis de algoritmos, el estudio de la complejidad y el diseño y verificación de programas y algoritmos y, más generalmente, la creciente algebraización de la teoría de la programación.

De este modo, sentimos la gran compenetración entre la matemática y la computación, ya sea debido al proceso de formalización y generalización que se está llevando a cabo en esta última, como a la utilización de resultados matemáticos como herramientas de trabajo, por ejemplo, el análisis de Fourier para resolver determinados problemas en tratamiento de imágenes, la teoría de funciones de variable compleja para el estudio de la complejidad algorítimica, la geometría en el diseño asistido o el álgebra abstracta en el diseño de software.

Otro aspecto que merece la pena destacar es la creciente proliferación de software destinado al trabajo en ámbitos concretos. Así tenemos los desarrollos de librerías de cálculo numérico y estadístico para lenguajes de programación muy utilizados, como ensamblador, C, Python, Java, Pascal, etc. Lenguajes como Hope y Miranda, destinados a programación funcional. Paquetes con lenguajes específicos adecuados a determinados entornos de trabajo, por ejemplo, el lenguaje R (o también, paquetes como SPSS, SYSTAT o RATS); paquetes con potentes capacidades numéricas como Octave (o también, MATLAB o Mathcad); programas destinados a la teoría de grupos como GAP (o también, Magma); calculadores simbólicos como Reduce o Maxima (o también, Derive), o librerías como SymPy para Python; y algunos otros de carácter más general, con un amplio espectro de usos poten-

ciales, como SageMath (o también, Mathematica, Maple, Theorist o Milo). Todo lo cual se convierte en una gran ayuda para la enseñanza, aprendizaje e investigación matemática.

§ 7.19 Lógica intuicionista

En línea con la constructibilidad que supone la computación, hemos de mencionar la *lógica intuicionista*[25]. En ella, un enunciado es verdadero cuando, y sólo cuando, se haya demostrado. La interpretación de Brouwer-Heyting-Kolmogorov (1934) es la siguiente[26]

0. $\bot$ no es demostrable;
1. una demostración de $p \wedge q$ consiste en una demostración de p y en una demostración de q;
2. una demostración de $p \vee q$ consiste en una demostración de p o en una demostración de q;
3. una demostración de $p \to q$ consiste en una construcción que transforma cualquier demostración de p en una demostración de q;
4. una demostración de $\exists x Px$ consiste en proporcionar un elemento a del dominio de interpretación (contexto, entorno, universo) y una demostración de Pa;
5. una demostración de $\forall x Px$ consiste en proporcionar una construcción que transforme cualquier demostración de que a está en el dominio de interpretación en una demostración de Pa.

Esta lógica admite siempre el principio de la no contradicción, $\neg(p \wedge \neg p)$, pero sólo admite el principio del tercio excluso, $p \vee \neg p$, a partir del momento en el que se haya encontrado una demostración para p, una demostración para su $\neg p$ o una demostración de que p no puede ser demostrado o de que $\neg p$ no puede ser demostrado. Como *reductio ad absurdum* depende del principio del tercio excluso, no admite aquélla cuando no admite éste. Ciertas fórmulas válidas tampoco se admiten siempre, por ejemplo, relaciones entre ambos principios, como las leyes de De Morgan.

Cuando p es una afirmación sobre los elementos de un conjunto finito, entonces es demostrable y, por tanto, se admite $\neg(p \wedge \neg p)$. También se admite la existencia de los números naturales y sólo se admite un infinito, el infinito potencial, el de los naturales. Se admite el principio de inducción.

[25] *Vid. v. gr.* https://en.wikipedia.org/wiki/Intuitionistic_logic.
[26] *Cfr. v. gr.* https://plato.stanford.edu/entries/intuitionism/.

§ 7.20 Propuesta de más actividades

Actividad 7.0

En estas notas, dos ejemplos de la estrategia constructiva aparecen en el teorema 13.21 (pág. 736 de esta edición) ($\aleph_0 < \mathfrak{c}$) y en el teorema 18.16 (pág. 957 de esta edición) (existencia de un número infinito de primos). Ambas, emplean, como marco la estrategia de reducción al absurdo.

0. Encontremos ejemplos en estas notas para todas las estrategias presentadas.
1. Aún más, en la diferente literatura que vayamos estudiando, ante una demostración, identifiquémosla como perteneciente a uno de estos tipos.

§ 7.21 Bibliografía

- Para una primera aproximación:

[62] María Manzano Arjona y Antonia Huertas Sánchez. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004.

[99] Amador Antón Antón y Pascual Casañ Muñoz. *Lógica matemática. II. Lógica de predicados*. NAU llibres, Valencia, España, 1998.

- Para estudiar, practicar y conocer más:

[64] Manuel Garrido Giménez. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

[65] Carmen García Trevijano. *El arte de la lógica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1999.

[122] Richard Hammack. *Book of proof*. Hammack, Richmond, Virginia, EE. UU., 3.ª ed., 2022.

[123] George Pólya. *Cómo plantear y resolver problemas*. Matemáticas. Trillas, Ciudad de México (MX-CMX), Estados Unidos Mexicanos, reimp. ed., 2008.

[124] Jiří Matoušek y Jaroslav Nešetřil. *Invitación a la matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2008.

- Para profundizar, acullá:

[66] Manuel GARRIDO GIMÉNEZ, Luis Manuel VALDÉS VILLANUEVA, Jesús MOSTERÍN DE LAS HERAS, Alfonso GARCÍA SUÁREZ y Carlos-Peregrín FERNÁNDEZ OTERO. *Lógica y lenguaje*. Cuadernos de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1989.

[67] Raymond Merrill SMULLYAN. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968).

[60] Herbert Bruce ENDERTON. *A mathematical introduction to logic*. Harcourt/Academic Press, San Diego, Condado de San Diego, California (US-CA), Estados Unidos de América, 2.ª ed., 2001.

Alexander BOGOMOLNY (https://es.wikipedia.org/wiki/Alexander_Bogomolny), *Cut the Knot* (https://www.cut-the-knot.org/), en particular, *Proofs in Mathematics* (https://www.cut-the-knot.org/proofs/index.shtml).

Capítulo 8

Éste no es el título de este capítulo

This was sometime a paradox, but now time gives it proof.
(William Shakespeare (1603) *Hamlet*, Acto III, Escena I, Línea 54).

Algunas situaciones singulares en lógica.

§ 8.0 Demostraciones, con lógica

Parece que una demostración debería asegurarnos lo afirmado en el ámbito donde haya sido demostrado, sin embargo puede que erremos en la misma afirmación (que no sea lo que perseguimos demostrar) o en la propia estructura de la demostración.

Ejemplo 259

Para el próximo reclutamiento, en la organización X deciden proponer dos pruebas estructuradas (quien entrevista proporciona una lista estable de cuestiones), que contienen cuestiones de respuesta de elección múltiple, cuestiones de profundidad (desarrollo de temas), cuestiones interactivas de descripción de conductas (¿qué haría la persona entrevistada en tal o cual supuesto o simulación?) y de tensión (que provocan a la persona aspirante al puesto de trabajo, inspeccionando su grado de paciencia). Lo novedoso, creen en la organización, es que el número de cuestiones lo determina quien aspira (esto mide su potencial de aceptación de riesgo, de atrevimiento). La dinámica de las pruebas es ir solicitando cuantas cuestiones deseen, se atrevan y se arriesguen a fallar.

La persona A, en la primera, solicita 6 (falla en la 6) y en la segunda, 19 (falla al principio 7 seguidas). La persona B, en la primera, solicita 14 (falla las 4, 9, 10) y en la segunda, 6. Es decir, los porcentajes de aciertos son los siguientes:

A: 5 de 6 en la primera prueba y 7 de 19 en la segunda;

B: 11 de 14 en la primera prueba y 2 de 6 en la segunda.

Entonces, si sólo se atiende a estos porcentajes,

- la persona A es preferida ($\succ$) a B en la primera prueba porque $5/6 > 11/14$ y también $A \succ B$ en la segunda prueba porque $7/19 > 2/6$;
- sin embargo, $B \succ A$ en el conjunto de ambas porque $13/20 > 12/25$.

Visto lo visto, ¿qué persona aspirante debe contratarse, la A o la B?

Resolución.— *¿Qué significa actuar lógicamente?* . . .

. . . *entre muchas cosas, tener sentido común y saber lo que se quiere.*

Y, por cierto, en este ejemplo, ¿se ha medido acaso lo que se pretendía, el atrevimiento, la actitud ante el riesgo de quien aspira al puesto? ■

§ 8.1 El paralogismo, la falacia y el sofisma

> En cuanto a declarar mis intenciones, soy la única persona que lo hace con tanta claridad y transparencia como yo.
>
> ([Sólo un ejemplo más]).

Las definiciones de paralogismo, falacia y sofisma, según el *Diccionario de la lengua española*° son las siguientes:

° Real Academia Española: *Diccionario de la lengua española*, 23.ª ed., [versión 23.6 en línea]. <https://dle.rae.es> [10.02.2023].

- `paralogismo`
  Del lat. tardío *paralogismus*, y éste del gr. παραλογισμός *paralogismós*, der. de παραλογίζεσθαι *paralogízesthai* 'paralogizar'.
  1. m. Razonamiento falso.

- `falacia`
  Del lat. *fallacia*.
  1. f. Engaño, fraude o mentira. *No lo creas, es una falacia*.

- `sofisma`
  Del lat. *sophisma*, y éste del gr. σόφισμα *sóphisma*.
  1. m. Razón o argumento falso con apariencia de verdad.

El paralogismo es un concepto lógico, meramente sintáctico, de la teoría de la demostración. Sofisma y falacia son conceptos semánticos, sociales, de uso. Una falacia es la expresión verbal, semántica, de un paralogismo. Un sofisma es una falacia con apariencia de no ser falacia, esto es, el sofisma supone engaño, la falacia, no.

Debido a esto y dado que no vamos a entrar en disquisiciones sobre intencionalidades, preferiríamos emplear la denominación neutra paralogismo, pues la esencia, en cualquier caso, está en que se trata de una argumentación o inferencia errónea.

Sin embargo, en el uso de la lengua, existen argumentos no sólidos, por lo que hablaremos de falacias. En general, distinguimos entre *falacias formales* y *falacias no formales*.

Existen múltiples taxonomías de falacias. Algunos de los ejemplos que siguen los categorizamos según la que denominamos taxonomía MBS, propuesta por la profesora Montserrat Bordes Solanas [125] —*vid. infra* Anexo (pág. 1454 de esta edición)—.

§ 8.1.0 Aristóteles y sus *Refutaciones sofísticas*

En el capítulo cuarto de su obra *Refutaciones sofísticas*, Aristóteles identifica y explica las siguientes *falacias «en función de la expresión»* (diríamos lingüísticas).

> A su vez, las cosas que provocan una (falsa) apariencia en función de la expresión son seis, a saber: la homonimia, la ambigüedad, la composición, la división, la acentuación y la forma de expresión.
>
> (Aristóteles, *Refutaciones sofísticas*, en *Tratados de Lógica (Órganon)*, 165b25).

Corresponden a las conocidas: falacia por equivocidad; falacia por anfibología; falacia por composición; falacia por división; falacia por énfasis, y falacia por forma de expresión (un tipo de falacia por ambigüedad).

- Una *falacia por equivocidad* corresponde a una ambigüedad semántica, léxica, y sucede cuando el significado de los términos involucrados en las premisas varía según éstas. Según la taxonomía MBS es una *falacia informal que contraviene el criterio de claridad*, subtipo *falacia dependiente del lenguaje* y, en concreto, una *falacia por ambigüedad* (MBS6.1.1 —*vid. infra* Anexo (pág. 1454 de esta edición)—).

Ejemplo 260

Digamos por qué son falacias por equivocidad las siguientes afirmaciones.

0. «El cubo es una operación de segundo orden, el cubo es un recipiente, luego un recipiente es una operación matemática».
1. «El conocimiento es poder, el poder es algo que corrompe, luego el conocimiento es algo que corrompe».

Resolución.—

0. La falacia se produce porque «cubo» tiene significados distintos en cada premisa.
1. La falacia se produce porque se ha alterado el significado de «es» (de expresar una identidad en la primera premisa a un uso predicativo en la segunda). ■

- Una *falacia por anfibología* corresponde a una ambigüedad sintáctica, estructural (o incluso semántica pero inmersa en una subestructura de la afirmación). Según la taxonomía MBS es una *falacia informal que contraviene el criterio de claridad*, subtipo *falacia dependiente del lenguaje* y, en concreto, una *falacia por ambigüedad* (MBS6.1.1 —*vid. infra* Anexo (pág. 1454 de esta edición)—).

Ejemplo 261

¿Es una falacia por anfibología la afirmación «Todo grupo tiene un elemento neutro, $(\mathbb{Z}, +)$ tiene por elemento neutro el 0, luego todo grupo tiene por elemento neutro el 0»?

Resolución.— Sí: el enunciado anfibológico es la primera premisa, pues en una interpretación el neutro puede ser distinto para cada grupo y en la otra (la que usa el argumento), todos los grupos tienen el mismo elemento neutro. ■

- Una *falacia por composición* sucede cuando se le atribuye una propiedad a un todo porque sus partes la tienen. Según la taxonomía MBS es una *falacia informal que contraviene el criterio de suficiencia*, concretamente, una *falacia mereológica* (MBS8.6 —*vid. infra* Anexo (pág. 1454 de esta edición)—).

Ejemplo 262

¿Es una falacia por composición la afirmación «Los ángulos internos de un heptágono valen menos de 900 grados, luego todos los ángulos internos de un heptágono [en conjunto, en suma] valen menos de 900 grados»?

Resolución.— Claramente, pues se le está atribuyendo la propiedad de valer 900 al conjunto de todos los ángulos internos por la sola razón de que cada ángulo interno lo satisface. ■

- Una *falacia por división* corresponde a atribuir una propiedad a las partes de un todo porque éste la tiene. Según la taxonomía MBS es una *falacia informal que contraviene el criterio de suficiencia*, concretamente, una *falacia mereológica* (MBS8.6 —*vid. infra* Anexo (pág. 1454 de esta edición)—).

Ejemplo 263

¿Es una falacia por división la afirmación «Todos los ángulos internos de un heptágono [en conjunto, en suma] valen 900 grados, luego cualquiera de ellos vale 900 grados»?

Resolución.— Claramente, pues se le está atribuyendo la propiedad de valer 900 a cada ángulo interno por el solo hecho de que el conjunto de todos los ángulos internos lo satisface. ■

- Una *falacia por énfasis* (o, sinónimamente, *falacia por acento*) ocurre cuando se destaca toda o parte de la afirmación, sea con la entonación o con pausas, o en lo escrito, utilizando comas, o incluso palabras en cursiva o mayúsculas.

Ejemplo 264

Qué más da decir «No es equivalente sumar y multiplicar» que decir «No, es equivalente sumar y multiplicar», ¿verdad?

Resolución.— Pues no, no da igual; la coma, ese pequeño cambio gramatical, hace que cambie el significado al destacar parte de la afirmación; se trata de una falacia por énfasis. ■

- Una *falacia por forma de expresión* (o, sinónimamente, *falacia por figura retórica*) ocurre cuando lo que es diferente se expresa con la misma forma.

Ejemplo 265

En la afirmación «Se trata de una sociedad emergente y fabricante», ¿nos referimos a dos cualidades inherentes de esa sociedad?

Resolución.— Las expresiones «emergente» y «fabricante» son de la misma forma —acaban en -ente—, pero mientras la primera es un adjetivo que denota una propiedad, condición o estado —algo que aparece, que surge—, la segunda es un sustantivo que denota una acción —no sólo que posea la cualidad de fabricar sino que realmente fabrica—; sin embargo, la expresión «la sociedad fabricante», usando fabricante como adjetivo, parece referirse más a una cualidad inherente a la sociedad que a la acción, a su función o actividad, que seguramente sería a lo que hubiésemos querido referirnos. ■

Para finalizar el capítulo cuarto de su obra *Refutaciones sofísticas*, Aristóteles identifica las siguientes *falacias «al margen de la expresión»* (diríamos no lingüísticas) y las explica en su capítulo quinto.

> Por su parte, las especies de razonamientos desviados, al margen de la expresión, son siete: primera, en función del accidente; segunda, decir de manera absoluta, o no absoluta sino bajo algún aspecto, o en algún sitio, o en alguna ocasión o respecto a algo; tercera, en función del desconocimiento de la refutación; cuarta, en función de la consecuencia; quinta, asumir la proposición que al principio se ha propuesto probar; sexta, poner como causa lo que no es causa, y séptima, convertir varias preguntas en una.
>
> (Aristóteles, *Refutaciones sofísticas*, en *Tratados de Lógica (Órganon)*, 166b20-25).

Corresponden a las conocidas: falacia por accidente; falacia por afirmación del consecuente; falacia por accidente inverso; falacias por *ignoratio elenchi*; falacia del círculo vicioso o «petitio principii»; falacias de la relación causa-efecto (*non causa pro causa*), y falacia de la pregunta compleja o *plurium interrogationum*.

- En una *falacia por accidente* (o, sinónimamente, *falacia por dicto secundum quid ad dicto simpliciter* o, a veces, *falacia de generalización inadecuada*) se toma lo particular como general (cosa que podría explicar que la muestra a partir de la que se pretende inferir la conclusión no fuese representativa de la población).

Ejemplo 266

Expliquemos por qué son falacias por accidente las siguientes afirmaciones.

0. «Algún número es mayor que cero, todo parámetro es número, luego todo parámetro es mayor que cero».
1. «Alguna bola es roja, esto es una bola, luego esto es una bola roja».

Resolución.—

0. Se realiza una generalización inadecuada, pues se confunde una propiedad particular de algunos números —ser mayores que cero— con una característica general de todos los números; existe el número cero y existen los números negativos y no hay ninguna información que los excluya de ser tenidos en cuenta.

1. De nuevo, se realiza una generalización inadecuada, pues de existir al menos una bola que tiene la propiedad de ser roja, esto es, de una característica arbitraria de una bola particular (el color en este caso) no puede inferirse, sin más información, que dicha característica la posean todas las bolas. ■

- En una *falacia por afirmación del consecuente* se infiere la verdad del consecuente a partir de la del antecedente. Es una *falacia formal*, en concreto una *falacia del condicional* (*vid. infra* Anexo (pág. 1454 de esta edición)—). Puede expresarse así:

$$\otimes \quad \begin{array}{l} A \rightarrow B \\ B \\ \hline A \end{array}$$

Ejemplo 267

Expliquemos por qué es una falacia por afirmación del consecuente la afirmación «Si estudio, aprobaré la asignatura. He aprobado la asignatura. Por lo tanto, estudié.».

Resolución.— Siendo $A \leftrightharpoons$ yo estudio, y $B \leftrightharpoons$ apruebo la asignatura, es una falacia porque puede suceder B sin necesidad de que suceda A, esto es, puede suceder que apruebe la asignatura sin estudiar, por birlibirloque. ■

- En una *falacia por accidente inverso* (o, sinónimamente, *dicto simpliciter ad dicto secundum quid*), se aplica una regla general a un caso particularmente excepcional.

Ejemplo 268

Demostremos que es una falacia por accidente inverso la afirmación «Las personas necesitan dormir entre siete y ocho horas cada noche para gozar de buena salud. Tú duermes sólo cinco horas al día. Por lo tanto, no debes gozar de buena salud».

Resolución.— La realidad es que no todas las personas requieren del mismo número de horas de sueño para gozar de buena salud. Esta argumentación es falaz por accidente inverso, pues aplica la regla general a tu caso sin tener en cuenta que tú puedes ser particularmente excepcional, una persona que a la que le basta y sobra con cinco horas de sueño cada noche. ■

- Una *falacia informal que contraviene el criterio de relevancia* (o, sinónimamente, falacia por *ignoratio elenchi* —por ignorancia de la refutación—) sucede cuando se presenta un argumento cuya conclusión no aborda el tema en cuestión.

Ejemplo 269

Dos personas debaten sobre la contaminación ambiental; A dice «Deberíamos reducir la contaminación ambiental», a lo que B responde «Pero, ¿cómo puedes decir eso si hay personas que no tienen trabajo?». Demostremos que B comete una falacia por *ignoratio elenchi*.

Resolución.— Sin duda, la falta de empleo es un problema relevante, sin embargo, abogar por su reducción como hace B, no responde a lo planteado por A, a saber, la reducción de la contaminación ambiental. ■

- Una *falacia del círculo vicioso* (o, sinónimamente, falacia por *petitio principii*) sucede en un argumento cuando alguna de sus premisas incluye la verdad de la conclusión.

Ejemplo 270

Demostremos que se comete una falacia por *petitio principii* al afirmar que «La belleza del arte radica en que toda obra de arte es bella».

Resolución.— Es que es un argumento circular, pues define la belleza del arte por la belleza de las obras de arte, pero éstas son arte, así que vuelta al principio. ■

- Una falacia de la relación causa-efecto (o, sinónimamente, falacia por *non causa pro causa*) sucede cuando se concluye que una cosa causa otra simplemente porque frecuentemente se presentan

asociadas —siendo la realidad que ambas cosas pudiesen coincidir o guardar correlación sin tener ninguna conexión causal—.

Ejemplo 271

Demostremos que se comete una falacia por *non causa pro causa* al afirmar que «Cada vez que toco madera cuando hablo de algo importante, las cosas salen bien. Por lo tanto, tocar madera es lo que hace que las cosas salgan bien».

Resolución.— Este argumento confunde la coincidencia con una relación causal; la realidad es que la práctica de tocar madera no tiene ningún efecto sobre cómo saldrán las cosas. ■

- Una de las formas de la *falacia de la pregunta compleja* (o, sinónimamente, *falacia «plurium interrogationum»*) corresponde a exigir una respuesta única a una pregunta múltiple.

Ejemplo 272

Demostremos que se comete una falacia de la pregunta compleja al preguntar «¿Dejó ya de intentar resolver la conjetura fuerte de Goldbach?».

Resolución.— En efecto, pues en realidad, «¿dejó ya de intentar resolver la conjetura fuerte de Goldbach?» es una pregunta doble, a saber, ¿ha intentado resolver la conjetura fuerte de Goldbach?, y de ser así, ¿dejó de intentarlo? ■

§ 8.1.1 Otras falacias formales

Destacamos algunas más.

- La *falacia por negación del antecedente* sucede cuando de la negación del antecedente se sigue la negación del consecuente. Es una *falacia formal*, en concreto una *falacia del condicional* (MBS5.3 —*vid. infra* Anexo (pág. 1454 de esta edición)—). Puede expresarse así:

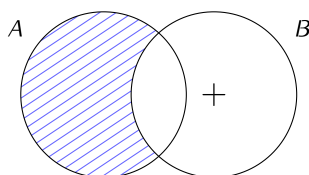
$$\otimes \quad \begin{array}{l} A \to B \\ \neg A \\ \hline \neg B \end{array}$$

Ejemplo 273

Demostremos que la falacia por negación del antecedente es, en efecto, una falacia.

[Cubit 51].

Resolución.— La siguiente es una demostración diagramática, con diagramas de VENN, del hecho de ser falacia:



muestra un contraejemplo: la zona rayada en azul, vacía, es precisamente lo que significa $A \to B$; la cruz indica que puede existir un ejemplar de $\neg A$ que es B; por lo tanto, no es posible afirmar que siempre $\neg A$ sea $\neg B$. ■

Ejemplo 274

Demostremos que se comete una falacia por negación del antecedente en el argumento «Si estuviese demostrada la conjetura de Goldbach, no habría que demostrar nada más en matemáticas, pero como la conjetura de Goldbach no está demostrada, hay que seguir demostrando cosas en matemáticas».

Resolución.— Siendo $A \leftrightharpoons$ La conjetura de Goldbach está demostrada, y $B \leftrightharpoons$ No hay que demostrar nada más en matemáticas, entonces su esquema argumental es justamente el visto de la falacia por negación del antecedente, pues $\neg A$ es «La conjetura de Goldbach no está demostrada» y $\neg B$ es «Aún hay que demostrar cosas en matemáticas». ■

Observación 8.1.0.— Aunque paralógico, el del anterior ejemplo es un razonamiento que pudiésemos considerar inductivamente fuerte, ya que es más probable que haya que seguir demostrando cosas en matemáticas si la conjetura de Goldbach no está demostrada que si lo estuviese (de hecho, si está demostrada, según la primera premisa, es seguro que no habría que demostrar nada más en matemáticas).

Actividad 8.0

Refutemos diagramáticamente, utilizando diagramas lógicos de VENN, la falacia de negación del antecedente.

- La *falacia ad logicam* (falacia de la falacia) (MBS5.6 —*vid. infra* Anexo (pág. 1454 de esta edición)—) es una *falacia formal* que se produce cuando por ser una argumentación falaz se asegura que su conclusión es falsa. Puede expresarse así:

$$\otimes \quad \begin{array}{l} A \to B \\ \text{«}A \to B\text{» es una falacia} \\ \hline \neg B \end{array}$$

Ejemplo 275

Has deducido erróneamente que sucede B a partir de que sucede A, por tanto, no sucede B.

Ejemplo 276

Demostremos que se comete una falacia *ad logicam* en el argumento «Paa dice que si estuviese demostrada la conjetura de Goldbach, no habría que demostrar nada más en matemáticas; también dice que como no está demostrada, hay que seguir demostrando cosas en matemáticas; pero esto es una falacia por negación del antecedente, así que sí, sí que hay que seguir demostrando cosas en matemáticas».

Resolución.— Pues no, que Paa cometa una falacia al decir todo lo que dice no implica ni que su conclusión sea verdadera ni que sea falsa. ■

- Una *falacia por vaguedad* (MBS6.1.2 —*vid. infra* Anexo (pág. 1454 de esta edición)—) sucede ante ciertos términos imprecisos, vagos.

Ejemplo 277

Demostremos que se comete una falacia por vaguedad en el argumento «Quitar alguna arena de este montón no va a hacer que deje de ser un montón de arena».

Resolución.— El sofisma se produce por la imprecisión de «alguna» respecto a la cantidad de arena (así como, eventualmente, respecto al número de veces que pueda repetirse la acción)[1]. ■

- Una *falacia por inducción precipitada* se produce cuando se generaliza a partir de una muestra no representativa de la población a la que se generaliza. Es una *falacia informal que contraviene el criterio de suficiencia*, concretamente una *falacia de la inducción o secundum quid* (MBS8.1 —*vid. infra*

[1] Léase sobre la *paradoja sorites* —*cfr. v. gr.* https://es.wikipedia.org/wiki/Paradoja_sorites.

Anexo (pág. 1454 de esta edición)—). Aunque se trata de una falacia informal, tiene su correspondiente en el ámbito formal y en lógica de primer orden pudiese expresarse así:

$$\otimes \quad \frac{\begin{array}{l}\exists a \\ Pa\end{array}}{\forall x Px}$$

Ejemplo 278

Demostremos que se comete una falacia por inducción precipitada en el argumento «Esta persona de esta organización es honrada, luego todas las personas de esta organización son honradas».

Resolución.— A no ser que la organización sea unipersonal, parece patente que no debiésemos inferir la honradez de todo el personal a partir de la honradez de una persona. ■

Y así pudiésemos seguir analizando aún más falacias formales, como, por ejemplo, las siguientes.

- Una *falacia por afirmación de la disyunción* se produce cuando se asume que si una disyunción es verdadera y uno de los disyuntos es verdadero, entonces el otro disyunto debe ser falso. En lógica de primer orden pudiese expresarse así:

$$\otimes \quad \frac{\begin{array}{l}A \lor B \\ A\end{array}}{\neg B}$$

Ejemplo 279

Demostremos que se comete una falacia por afirmación de la disyunción en el argumento «Tengo los brazos cruzados o estoy esperando el autobús. Tengo los brazos cruzados. Luego, no estoy esperando el autobús».

Resolución.— Esto es incorrecto, pues podemos estar esperando el autobús y tener los brazos cruzados. ■

- Una *falacia por falso dilema* (*B&W Thinking*) sucede cuando se presenta una situación como si solo hubiera dos opciones posibles, ignorando otras alternativas. En lógica de primer orden pudiese

expresarse así:

$$\otimes \quad \frac{\begin{array}{l} A \vee B \vee C \\ \neg A \end{array}}{B}$$

Ejemplo 280

Demostremos que se comete una falacia por falso dilema en el argumento «O estás conmigo o estás contra mí».

Resolución.— Este argumento asume que existen únicamente dos opciones excluyentes, esto es, ignora la posibilidad de que alguien pueda tener una posición intermedia, ser neutral o simplemente que no quiera expresar su opinión o elección; de ahí la falacia. ■

- Una *falacia por cuatro términos* (*quaternio terminorum*) sucede cuando un silogismo tiene cuatro (o más) términos en lugar de los tres requeridos, lo que lo hace inválido.

Ejemplo 281

Demostremos que se comete una falacia por cuatro términos en el argumento «Todo león es un animal. Esta estatua es un león. Por tanto, esta estatua es un animal».

Resolución.— En este silogismo, los términos son 'león' (animal), 'animal', 'estatua' y 'león' (estatua); precisamente la introducción de este cuarto término hace que el silogismo sea inválido. Formalmente, pudiésemos explicitar la existencia de dominios disjuntos D_A (animal) y D_M (mineral), de manera que la premisa mayor es $\forall x \in D_A(L(x) \rightarrow A(x))$, la menor es $L(e)$ $(e \in D_M)$, de donde no es aplicable la mayor, ya que $D_A \cap D_M = \emptyset$, por lo que la conclusión $A(e)$ no es válida (es un sinsentido afirmar que una estatua es un animal). ■

- Una *falacia por no universalidad del término medio* (o, sinónimamente, *falacia del medio no distribuido*) sucede cuando el término medio en un silogismo no se distribuye universalmente en ninguna de las premisas. En lógica de primer orden pudiese expresarse así:

$$\otimes \quad \frac{\begin{array}{l} \forall x(Px \rightarrow Mx) \\ \forall x(Sx \rightarrow Mx) \end{array}}{\forall x(Sx \rightarrow Px)}$$

Ejemplo 282

Demostremos que se comete una falacia por no universalidad del término medio en el argumento «Todas las mujeres tienen derechos y obligaciones. Todos los hombres tienen derechos y obligaciones. Luego, todos los hombres son mujeres».

Resolución.— En este silogismo, el término medio 'tener derechos y obligaciones' no se distribuye universalmente en ninguna de las premisas —formalmente, la premisa mayor es $\forall x(Hx \to Dx)$ y la menor es $\forall x(Mx \to Dx)$, donde $Hx \leftrightharpoons x$ es hombre, $Dx \leftrightharpoons x$ tiene derechos y obligaciones, y $Mx \leftrightharpoons x$ es mujer—. ■

Observación 8.1.1.— Por la distribución cuantorial, todos universales, pudiese pensarse en el modo Barbara de la primera figura, en cuyo caso la premisa mayor debiese tener la estructura M-P y no P-M como aquí; por otra parte, por la distribución de S, P y M, pudiese pensarse en la segunda figura, pero no se corresponde con ninguno de los modos válidos de ésta (Cesare, Camestres, Festino y Baroco).

- Una *falacia por transposición de cuantor* sucede por un intercambio incorrecto de la cuantificación. En lógica de primer orden pudiese expresarse así:

$$\otimes \quad \frac{\forall x \exists y Pxy}{\exists y \forall x Pxy}$$

Ejemplo 283

Demostremos que se comete una falacia por transposición de cuantor en el argumento «Toda persona tiene un libro preferido. Luego, existe un libro que es el preferido de toda persona».

Resolución.— Claramente, las personas tenemos gustos diferentes: el hecho de que toda persona tenga un libro preferido no implica que haya un único libro que sea el preferido de toda persona. ■

- La *falacia del existencial* sucede cuando se infiere la existencia de un objeto de un dominio a partir de una afirmación universal, sin evidencia alguna de que dicho dominio sea no vacío; es precisamente cuando el dominio es vacío cuando se produce la falacia. En lógica de primer orden

pudiese expresarse así:

$$\otimes \quad \frac{\forall x Px}{\exists x Px}$$

Ejemplo 284

Demostremos que se comete una falacia del existencial en el argumento «Todos los unicornios tienen un cuerno en la frente, luego existe un unicornio que tiene un cuerno en la frente».

Resolución.— La falacia surge de asumir por la afirmación universal la existencia de unicornios, cuando en nigún momento aquélla establece dicha existencia. ■

§ 8.1.2 Falacias no formales materiales

Entre las *falacias no formales* distinguimos las *falacias por ambigüedad* y las *falacias materiales*.

De las primeras, ya hemos hablado en ejemplo 8.1.0 (pág. 496 de esta edición). Entre las falacias materiales distinguimos: las *falacias por datos insuficientes* y las *falacias de pertinencia*.

Falacias por datos insuficientes

- En una *falacia de falta de pruebas* (o, sinónimamente, *falacia de evidencia incompleta*) se omiten intencionadamente los datos o hechos desfavorables para la conclusión.

  Ejemplo 285

  A la hora de adquirir una cámper se destacan sus comodidades y su buen consumo, pero no se dice nada de su peor manejabilidad debido a su tamaño.

- En una *falacia de falsa causa* se toma un hecho como causa de otro, cuando no lo es.

  Entre las falacias de falsa causa se distinguen la de correlación coincidente y la de correlación accidental.

  - Una *falacia de correlación coincidente o «post hoc»* (o, sinónimamente, *post hoc, ergo propter hoc* [tras esto, luego a causa de esto] —o, simplemente, *post hoc*— o *non sequitur* [no le sigue]) (MBS8.2.3 —*vid. infra* Anexo (pág. 1454 de esta edición)—):

    $$\{\text{ Sucede } A, B \text{ sucede después de } A\} \vdash A \text{ es causa de } B \ ^{\otimes}.$$

Ejemplo 286

Tras ponerse una vacuna, una persona tiene un problema de salud y lo achaca a haberse vacunado.

- Una *falacia de correlación accidental* —«non causa pro causa» (una no causa por causa):

$$\{A \text{ sucede cuando } B \text{ sucede}\} \vdash A \text{ es causa de } B \text{ o } B \text{ es causa de } A\ ^{\otimes}.$$

Ejemplo 287

Siempre que marcho a casa del trabajo, veo mucho tráfico en las carreteras; por lo tanto, mi ida a casa desde el trabajo causa el incremento de tráfico en las carreteras.

Falacias de pertinencia

- «*Ad hominen*» («contra el hombre»): se afirma la falsedad de lo afirmado por una entidad por el simple hecho que lo ha afirmado dicha entidad; existen dos modalidades:
  - *Ofensiva*:

$$\{\text{«}A \text{ afirma } P\text{», «}A \text{ no es digna de consideración por tal y cual»}\} \vdash P \text{ es falso}\ ^{\otimes}.$$

  - Circunstancial:

$$\{\text{«}A \text{ afirma } P\text{», «}A \text{ no es fiable por sus circunstancias particulares»}\} \vdash P \text{ es falso}\ ^{\otimes}.$$

- «*Ad baculum*» («al bastón»), apelación a la fuerza:

$$\{A \text{ afirma } P, A \text{ tiene dominio sobre } B\} \vdash P\ ^{\otimes}.$$

- «*Ad populum*» («al pueblo»): Se excitan los sentimientos del contrario a favor de la afirmación (dependiendo del tipo de sentimiento que se excite puede recibir otros nombres, por ejemplo «Ad misericordiam» —«a la misericordia»—):

$$\{A \text{ afirma } P, \text{Se apela (sin fundamento) a los sentimientos y emociones de } A \text{ sobre } P\} \vdash P\ ^{\otimes}.$$

- «*Ex populo*» («a partir del pueblo»): Se apela (sin fundamento) a la creencia de una mayoría:

$$\{\text{Se afirma } P, \text{La mayoría cree } P\} \vdash P\ ^{\otimes}.$$

- «*Ad verecundiam*» («apelación a la autoridad»):

$$\{A \text{ afirma } P, \text{Se apela (sin fundamento) al conocimiento de } A \text{ sobre } P\} \vdash P \ ^{\otimes}.$$

- «*Ad ignorantiam*» («a la ignorancia»): Si no se ha demostrado la falsedad de algo se infiere que es verdadero:

$$\{\text{No existe prueba de que } P \text{ sea falso (respág. verdadero)}\} \vdash P \text{ es verdadero (respág. falso)} \ ^{\otimes}.$$

- «*Ignoratio elenchi*» («ignorancia del tema»): La conclusión que se obtiene no es o no tiene que ver con la premisa:

$$\{A \text{ afirma } P\} \vdash Q \ ^{\otimes}.$$

- «*Tu quoque*» («tú también»): Se devuelve la ofensa pretendiendo la razón (puede verse como un caso particular de sofisma «ad hominen»):

$$\{A \text{ afirma que } B \text{ satisface } P \text{ (algo negativo)}, B \text{ afirma que } A \text{ satisface } P\} \vdash B \text{ satisface } \neg P \ ^{\otimes}.$$

- «*Petitio principii*» («petición de principio»): La conclusión es una de las premisas:

$$\{P, P \rightarrow Q, Q \rightarrow P\} \vdash P \ ^{\otimes}.$$

§ 8.2 Creencia en la verdad

En lógica bivalente, el valor de verdad de una fórmula bien formada (fbf), $\phi(x_0, x_1, \ldots, x_n)$, está determinado dada una interpretación (una valoración de verdad para todas las variables x_i). Caso contrario, hablamos de *creencia*[2].

En ausencia total de información, nuestra creencia en un literal[3] es $1/2$, puesto que existen dos asignaciones posibles de verdad: 0 y 1. Sean p y q dos literales, tales que $p \neq q$ y $p \neq \neg q$. Si pensamos en $p \wedge q$, es $1/4$, puesto que existen cuatro asignaciones posibles de verdad y sólo una es 1. En el caso de $p \vee q$, es $3/4$, pues de las cuatro asignaciones posibles de verdad, tres hacen verdadera $p \vee q$.

[2] *Vid.* León Rojas [1] (§18.2 [pág. 458]).

[3] Recordemos: una fórmula bien formada (fbf) λ es un *literal*, precisamente si λ es una proposición atómica, o $\lambda \equiv \neg p$, siendo p una proposición atómica; una fbf es una $\wedge$-*cláusula* (*cubo*), precisamente si es un literal o una conjunción de literales; una fbf es una $\vee$-*cláusula*, precisamente si es un literal o una disyunción de literales; una fbf está en *forma normal conjuntiva* (FNC), precisamente si es tautología, contradicción, una $\vee$-cláusula o una conjunción de $\vee$-cláusulas; una fbf está en *forma normal disyuntiva* (FND), precisamente si es tautología, contradicción, una $\wedge$-cláusula o una disyunción de $\wedge$-cláusulas.

Nuestra creencia en $p \rightarrow p \lor q$ es la total seguridad, pues de las cuatro posibles asignaciones de verdad, las cuatro la hacen verdadera.[4]

Sabemos que es seguro que toda fbf puede transformarse en una fbf equivalente en forma normal conjuntiva (FNC), esto es, una conjunción de cláusulas, donde cada cláusula es una disyunción de literales, y cada literal es una variable atómica o su negación:

$$\begin{aligned}\phi(x_0, x_1, \ldots, x_n) &= c_0 \land c_1 \land \ldots \land c_n \\ &= (l_{0,0} \lor l_{0,1} \lor \ldots \lor l_{0,k_0}) \land \ldots \land (l_{n,0} \lor l_{n,1} \lor \ldots \lor l_{n,k_n})\end{aligned}$$

Abreviadamente:

$$\phi(x_0, x_2, \ldots, x_n) = \bigwedge_{i=0}^{n} \bigvee_{j=0}^{k_i} l_{i,j}$$

ocurriendo que $(\forall i)(\forall j)(\exists k)(l_{i,j} = x_k \lor l_{i,j} = \neg x_k)$.

Teorema 8.0

Careciendo de cualquier información, la creencia en $\phi(x_0, x_1, \ldots, x_n)$ es:

$$1 - \frac{2^{a_0} + 2^{a_0+a_1+1} + 2^{a_0+a_1+a_2+2} + \ldots + 2^{a_0+a_1+\ldots+a_n+n} - 1}{2^{k_0+k_1+\ldots+k_n}}$$

siendo:

$$\begin{cases} a_0 = k_0 \\ a_{i+1} = k_{i+1} - k_i - 1 \quad (0 \leq i < n). \end{cases}$$

Pudiese atraernos la idea de construir una lógica de n valores de creencia; por ejemplo, una de cinco valores de creencia con los cinco valores aportados por $\perp$ (0), $p \land q$ (1/4), $p \leftrightarrow q$ (1/2), $p \lor q$ (3/4) y $\top$ (1). En el siguiente capítulo veremos cómo se ha hecho pero trabajando con valores de verdad: las lógicas multivalentes[5].

Por otra parte, este contexto de creencia puede ayudarnos a resolver alguna que otra *paradoja*[6].

Ejemplo 288

Una paradoja clásica, de Russell (1901) —*cfr.* Mosterín [126] (págs. 152ss.)—: pensemos en aquél barbero que afeita únicamente a aquéllos que no se afeitan a sí mismos; entonces, ¿quién afeita al barbero?

[4] Esta creencia es llamada en otros textos *densidad de verdad* (*cfr. v. gr.* https://crypto.stackexchange.com/questions/87613/earliest-citation-for-truth-density).

[5] *Cfr. infra* cuadro 9 (pág. 516 de esta edición).

[6] Acerca de las paradojas, *vid. v. gr.*: https://en.wikipedia.org/wiki/Paradox, y https://plato.stanford.edu/entries/paradoxes-contemporary-logic/.

Resolución.— El presente contexto de creencia aporta una posible resolución de esta paradoja,pues todo cobra sentido si V es una valoración de creencia en vez de una valoración de verdad: sea $S \equiv$«El barbero se afeita a sí mismo»; el valor de verdad de esta proposición es 0 ó 1; carecemos por completo de información, ya que la circularidad $S \to \neg S \to S$, y el hecho de ver al barbero afeitado, no aportan información alguna; por esto, nuestra creencia en que suceda se reparte por igual entre S y $\neg S$: $V(S) = V(\neg S) = 1/2$, esto es, creemos en la misma medida que el barbero se afeita a sí mismo como que no se afeita a sí mismo. ■

Conciencia de la autoconciencia

Con el nombre de *lógica doxástica*[*] conocemos aquélla en la que nos preocupamos de formalizar el razonamiento acerca de nuestras creencias. Algunos de los tipos de razonadores que define Raymond Merrill SMULLYAN son[†]:

Razonador de tipo 1.— Cree todas las tautologías y para cualesquiera proposiciones X e Y, si cree X y cree $X \to Y$, entonces cree Y. Además, si llega a saber algo, entonces sabe que lo sabe.

Razonador presumido (*conceited*).— Cree que siempre acierta en sus juicios.

Razonador peculiar.— Dos tipos: un razonador certero (*accurate*) con respecto a p precisamente si el hecho de que el razonador crea p implica que p es verdadera; en otras palabras, si no se da el caso de que crea p, o se da el caso de que crea p y p es verdadera; el razonador es desacertado con respecto a p si cree p y p es falsa.

Observación.— Por Bp y Cp entenderemos: $Bp \leftrightharpoons R$ cree o creerá p; $Cp \leftrightharpoons Bp \wedge p$ (esto es, R cree correctamente p).

Razonador regular.— Razonador tal que sean cuales sean p y q, si cree $p \to q$, entonces cree $Bp \to Bq$.

Razonador de tipo 1*.— De tipo 1 y regular.

Observación.— Para un razonador de tipo 1, si cree $p \to q$, entonces $Bp \to Bq$ es verdadera; para un razonador de tipo 1* en la misma situación, $Bp \to Bq$ no sólo es verdadera, sino que además cree correctamente $Bp \to Bq$.

Razonador de tipo 2.— De tipo 1 sucediendo además que cree todas las proposiciones de la forma $(Bp \wedge B(p \to q)) \to Bq$.

Observación.— La proposición $(Bp \wedge B(p \to q)) \to Bq$ es verdadera para un razonador de tipo 1, sin embargo dicho razonador no conoce necesariamente que esta proposición es verdadera.

Razonador normal.— Si sucede que para toda p, si cree p, entonces cree Bp (cree que cree p).

Razonador de tipo 3.— De tipo 2 y normal.

Razonador de tipo 4.— De tipo 3 y cree (sabe) que es normal.

Observación.— La proposición $Bp \to BBp$ es verdadera para un razonador normal, sin embargo dicho razonador no conoce necesariamente que esta proposición es verdadera, por lo que no tiene medios de creer (saber) que es normal. Esto sucede para un razonador de tipo 3. Pero un razonador de tipo 4 cree $Bp \to BBp$, en otras palabras, cree (sabe) que es normal.

Teorema.—[Conciencia de la autoconciencia] Un razonador de tipo 4 sabe que lo es.

La cuestión es, ¿nos guía esto hacia la formalización de la *conciencia artificial*[*]? Porque urge, un grave problema que enfrentará la seguridad en breve es el siguiente: ¿superará un ser humano siempre la prueba de convencer a una inteligencia artificial de que es un ser humano?

[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/Doxastic_logic.
[†] *Cfr.* SMULLYAN, Raymond Merrill, *Forever Undecided. A puzzle guide to Gödel*, Alfred A. Knopf, Nueva York, 1987.
[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/Artificial_consciousness.

Dualismo

El *dualismo* es una corriente filosófica que propone que el origen y la naturaleza del universo se deben a la acción conjunta de dos sustancias primarias, la materia y el espíritu. Establece que las personas estamos formadas por un cuerpo y una mente que deben actuar conjuntamente. El cuerpo no actúa solo, sino que también lo hace con la mente, no se separan.[*]

Contrario a este principio se encuentra el *monismo*, el cual propone que sólo hay una sustancia primaria en el universo, materia o espíritu, ya seamos de tendencia materialista o ideológica.[†]

En semejanza a estos pensamientos tenemos las dos vertientes sobre el inicio del universo: hay quienes defienden que fue Dios la causa de este origen, y quienes proponen que es causa de la materia formada en una primera explosión (big bang) o incluso «anteriormente».

Y para quien lee, ¿dónde piensa que reside la inteligencia, en el cerebro o en la mente? ¿Y la conciencia? ¿Dónde piensa que se encuentra la esencia de la persona?, ¿en el cuerpo?, ¿en el alma?, ¿o quizás es fruto de la interrelación entre ambas?

[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/Dualism.
[†] *Vid. v. gr.* https://en.wikipedia.org/wiki/Monism.

No son éstas las notas donde discutir en profundidad los beneficios y perjuicios de la inteligencia artificial y de los artefactos robots pululantes. Aquí, en ellas, me quedo:

- en la *convivialidad*[7] propugnada por Iván ILLICH y, en particular, con estas palabras en *Deschooling Society*[8]:

  > Rodeado de herramientas todopoderosas, el hombre queda reducido a una herramienta de sus herramientas / Surrounded by all-powerful tools, man is reduced to a tool of his tools.

- con este pie de foto en *The Random House Encyclopedia*[9]:

  > Una persona y una caja registradora suman juntas el coste de cada artículo comprado. Algunas máquinas calcularán e incluso darán el cambio e imprimirán un recibo.

  si bien la proliferación de automatismos sustituidores de humanos, como cajeros automáticos, lugares de autoservicio, cajas automáticas de autocobro, etc., llaman irremediablemente a la reflexión inmediata, y

- con estas palabras de Sherry TURKLE en *En defensa de la conversación*[10]:

  > Yo había estado llevando robots diseñados para actuar como compañeros de los ancianos a residencias y a domicilios de ancianos que vivían solos. Quería explorar las posibilidades de la tecnología. Un día vi a una anciana que había perdido a un hijo hablando con un robot que tenía forma de bebé foca. Parecía que le miraba a los ojos. Parecía que seguía la conversación. La reconfortaba. A muchos miembros de mi equipo de investigadores y muchos de los empleados de la residencia les pareció algo asombroso.
  >
  > Esta mujer estaba intentando recuperarse de su pérdida con una máquina capaz de ofrecer una gran actuación. Y somos vulnerables: la gente experimenta incluso la empatía fingida como real. Pero los robots no son capaces de sentir empatía. No se enfrentan a la muerte ni conocen la vida. Así que cuando esta mujer halló consuelo en su compañero robot, a mí no me pareció asombroso. Sentí que habíamos abandonado a la mujer. Ser parte de esta escena fue uno de los momentos más desgarradores de mis quince años de investigación sobre robótica sociable.
  >
  > »Para mí fue un punto de inflexión: sentí el entusiasmo de mi equipo y de los empleados y los asistentes. En aquel lugar había mucha gente capaz de ayudar, pero todos nos apartamos, nos convertimos en una sala llena de espectadores, que solo estaban allí con la esperanza de que una anciana se encariñara con una máquina. Me pareció que todos estábamos contribuyendo a externalizar lo que los seres humanos hacemos mejor: comprendernos los unos a los otros, cuidarnos los unos a los otros.
  >
  > Esa experiencia que viví en la residencia de ancianos me preocupó, me perturbó pensar en *cómo hemos permitido que nos dejen en segundo plano, que un robot que no comprende nada nos convierta en meros espectadores*[11].

[7] *Vid. v. gr.* https://en.wikipedia.org/wiki/Conviviality.
[8] *Vid. Deschooling Society* (https://archive.org/details/DeschoolingSociety: pág. 76).
[9] *Vid. The Random House Encyclopedia*, 3.ª ed., 1990, pág. 1447.
[10] *Vid. En defensa de la conversación*, trad. Joan Eloi ROCA, Ático de los libros, p. 462.
[11] La cursiva es mía.

CAPÍTULO 9

Lógicas multivalentes

«Las personas que piensan en español (sic) sienten que “la incertidumbre es insoportable” y no tienen nada que hacer desde el punto de vista lógico, sin embargo, para una persona que piensa en Aymara, “ina” [quizás sí quizás no] forma parte de la realidad, y es tan lógico como “jisa” [sí] o “jani” [no]. Si ŁUKASIEWICZ hubiese sido un Quoya, probablemente hubiese considerado la lógica bivalente de los hispanohablantes tan extraña y digna de estudio como lo es la lógica polivalente.»

(Iván GUZMÁN DE ROJAS [127], cap. 3: The trivalent logic of Aymara).

Tras el embotamiento de lo bivalente y su parca expresividad, no perdamos la esperanza de tener alguna vez tiempo e inquietud para emprender el redescubrimiento de la fluidez perdida.

Podrían considerarse entre los primeros esbozos de formalización de una «lógica multivalente» aquellos intentos de Ramón LULL (aprox. 1232-1316) y Nicolás de KREBS (Nicolás de Cusa, 1401-1464).° Aunque, ya en ello, también pudiésemos remontarnos hasta ARISTÓTELES, con la discusión de las proposiciones que no lo son pero sí están, no se les puede asignar un valor de verdad, pero pueden enunciarse, y se vive con ellas, como por ejemplo: «mañana llueve»; o sea, la noción de verdad potencial.

° *Cfr.* PEÑA [128] (pág. 323).

§ 9.0 Lógicas trivalentes

Fue Charles Sanders PEIRCE (1839–1914), quien, hasta donde sabemos[1], formaliza por primera vez una lógica trivalente, con su idea de la *matemática triádica*, extensión de la clásica, en la que el *principio del tercio excluso* ($p \vee \neg p \equiv 1$) no es del todo verdadero —él distingue entre lo verdadero, lo falso, y lo que está en el *límite*—[2]. Parte de este trabajo no publicado, y realizado sobre 1909, está recogido en la obra de Nicholas RESCHER [129] (págs. 4–5).

El matemático ruso Nikolái Aleksándrovich VASÍLIEV, a partir de 1909, publica una serie de artículos en los que elabora una lógica trivalente, por eliminación del principio del tercio excluso, en la que las proposiciones podían ser «afirmativas», «negativas» o «indiferentes»; él la llama «lógica no aristotélica» [3]. El primer sistema desarrollado de lógica trivalente data de 1920 y es de Jan ŁUKASIEWICZ. Otros sistemas trivalentes son los de Emil Leon POST[4] (1921) [132], Stephen Cole KLEENE (1938) [133] —*et* [134] (pág. 334)—, Dmitry Anatol'evich BOCHVAR (1939) [135], Arend HEYTING (1956) [136], Hans REICHENBACH (1944) [137], y algunos otros —*cfr. infra* cuadro 9.0 (pág. 517 de esta edición)—. Parece ser que fue Mordchaj WAJSBERG (1931) [138] quien proporcionó la primera axiomatización de la lógica trivalente.

		ŁUKASIEWICZ				KLEENE (fuertes)				BOCHVAR				HEYTING				REICHENBACH			
p	q	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$	$\wedge$	$\vee$	$\rightarrow$	$\leftrightarrow$
0	1/2	0	1/2	1	1/2	0	1/2	1	1/2	1/2	1/2	1/2	1/2	0	1/2	1	0	0	1/2	1	1/2
1/2	0	0	1/2	1/2	1/2	0	1/2	1/2	1/2	1/2	1/2	1/2	1/2	0	1/2	0	0	0	1/2	1/2	1/2
1/2	1/2	1/2	1/2	1	1	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1	1	1/2	1/2	1	1
1/2	1	1/2	1	1	1/2	1/2	1	1	1/2	1/2	1/2	1/2	1/2	1/2	1	1	1/2	1/2	1	1	1/2
1	1/2	1/2	1	1/2	1/2	1/2	1	1/2	1/2	1/2	1/2	1/2	1/2	1/2	1	1/2	1/2	1/2	1	1/2	1/2

Cuadro 9.0.—Algunas lógicas trivalentes. Sólo aparece el tratamiento del nuevo valor de verdad $1/2$, pues todas ellas coinciden con la lógica clásica si $p, q \in \{0, 1\}$.

[1] *Cfr.* PEÑA [128] (págs. 323ss.).

[2] No obstante, José FERRATER MORA asegura que hay evidencias de que Guillermo de OCKHAM (1298–1349) hubiese sugerido ya el uso de tres valores de verdad. (Guillermo de OCKHAM es a quien le es atribuida la ley o *principio de parsimonia* (*navaja de* OCKHAM): las entidades no deben multiplicarse más allá de lo necesario, esto es, ante una situación o problema, deberíamos buscar explicaciones o soluciones construidas con el menor conjunto posible de elementos).

[3] José FERRATER MORA nos comenta el hecho de que VASÍLIEV hizo algo parecido con la lógica bivalente, a lo que había hecho Nikolai Ivanovich LOBACHEVSKY con la geometría euclidea; si bien, este último eliminó el axioma de las paralelas, VASÍLIEV eliminó la ley del tercio excluso —*cfr.* FERRATER MORA [130]; FERRATER MORA y LEBLANC [131].

[4] En realidad, la lógica desarrollada por Emil Leon POST, en 1921, posee un número indeterminado $n > 2$ de valores; además, se trata de una lógica de conjuntos de enunciados, y no de enunciados.

En las lógicas trivalentes es frecuente notar por 0, $1/2$ (o, sinónimamente, ?) y 1 la falsedad, la incertidumbre y la certeza y decir de un enunciado p que es falso, incierto (o posible) y verdadero, respectivamente. También es frecuente definir la interpretación de la negación de una proposición p como $1 - I(p)$, esto es, $I(\neg 0) = 1$, $I(\neg 1/2) = 1/2$ e $I(\neg 1) = 0$.

Otros dos operadores lógicos son mín y máx:

mín	0	1/2	1
0	0	0	0
1/2	0	1/2	1/2
1	0	1/2	1

máx	0	1/2	1
0	0	1/2	1
1/2	1/2	1/2	1
1	1	1	1

Como podemos apreciar, mín y máx son generalizaciones de $\wedge$ y $\vee$ de la lógica binaria. Como curiosidad, sepamos que también cumplen las leyes de De Morgan; de hecho, se pueden extender a cualquier número de valores de verdad y las seguirán cumpliendo. Sin embargo, estos operadores no son suficientes: hay funciones lógicas ternarias que no se pueden representar sólo con estos tres operadores básicos $\neg$, mín y máx.

Estas lógicas no satisfacen ni el *principio de contradicción* ($p \wedge \neg p \equiv \bot$) —ya que p y $\neg p$ pueden tener el mismo valor de verdad, $1/2$— ni el *principio del tercio excluso* ($p \vee \neg p \equiv \top$) —pues sí existe una tercera posibilidad, a saber, p puede ser incierto— ni tampoco otras fórmulas válidas de la lógica bivalente.

Si bien el principio de contradicción no se satisface, sí que es una fórmula válida en la lógica de Łukasiewicz: $p \leftrightarrow \neg\neg p$.

Actividad 9.0

¿Por qué no? Pudiésemos demostrar que $p \leftrightarrow \neg\neg p$ es una fórmula válida en la lógica de Łukasiewicz y, de paso, preguntarnos qué ocurre en las otras lógicas trivalentes expuestas.

Salvo en la lógica de Bochvar, existen, pues, las fórmulas insatisfactibles (siempre exactamente falsas), las fórmulas válidas (siempre exactamente verdaderas) y las incertidumbres (o posibilidades) (nunca falsas ni verdaderas). El hecho de que la lógica trivalente de Bochvar no contenga ni fórmulas válidas (debido a que todas sus primitivas producen $1/2$ si al menos uno de los argumentos asume tal valor) ni fórmulas insatisfactibles, hizo que surgieran los conceptos de cuasi fórmula válida y cuasi fórmula insatisfactible.

Definición 9.0.— Una fórmula es una *cuasi fórmula válida* si todos sus literales son distintos de 0.

Definición 9.1.— Una fórmula es una *cuasi fórmula insatisfactible* si todos sus literales son distintos de 1.

Ternaria: aritmética e implementación física

La *aritmética ternaria balanceada* es un sistema de numeración posicional que utiliza los dígitos $\{-1, 0, +1\}$. Las bases balanceadas tienen la ventaja de que pueden expresar números positivos y negativos sin necesidad de usar un signo. Por ejemplo:

...	-4	-3	-2	-1	0	+1	+2	+3	+4	...
...	$\underline{1}\underline{1}$	$\underline{1}0$	$\underline{1}1$	$\underline{1}$	0	1	$1\underline{1}$	10	11	...

Negar un número es tan sencillo como negar cada dígito individual. Las tablas de suma y multiplicación también son bastante sencillas.*

Matemáticamente se dice que la base 3 es la más eficiente para representar números. Una medida básica de la eficiencia de una base se mide como el producto del número de valores por el número de dígitos necesarios para representar un número cualquiera. Cuanto menor es este valor, más eficiente es la base. La base más eficiente posible es e, pero no parece que usar un número irracional como base sea muy práctico. El 3 es el entero más cercano y cumple con lo esperado.†

En cuanto a su implementación física, digamos que en los años 50 del siglo XX se construyó el computador ternario Setun‡, en la universidad de Moscú. Al parecer, era más eficiente y barato que las alternativas binarias, aunque fue abandonado con el tiempo. Aún así se ha seguido investigando el tema. Con respecto al diseño de circuitos de computación ternaria, pudiese partirse de la computación binaria (CMOS), pues cambiando la tensión de la base de los transistores P (PMOS) a -Vdd, obtenemos las puertas ternarias NOT, MIN y MAX (que operan así con tres niveles de tensión -Vdd, 0 y +Vdd, representando tres valores lógicos).

* *Vid. v. gr.* https://en.wikipedia.org/wiki/Balanced_ternary.
† *Vid. v. gr.* https://en.wikipedia.org/wiki/Optimal_radix_choice.
‡ *Vid. v. gr.* https://en.wikipedia.org/wiki/Setun.

§ 9.1 Lógicas polivalentes

Si en vez de tres valores de verdad admitimos $n \in \mathbb{Z}^+$, entonces estamos ante una lógica polivalente (tetravalente, pentavalente, hexavalente, . . ., enevalente) —si bien lo que signifique cada uno de los valores de verdad vendrá en función del contexto, aunque, en general, expresan un grado de verdad o certeza, desde la falsedad (0) a la verdad (1), pasando por la ignorancia absoluta (que designaremos por $1/2$) (u otra interpretación, como la indiferencia).

Teorema 9.0
El número de funtores veritativos kádicos en una lógica enevalente es n^{n^k}.

A modo de ejemplo, el siguiente cuadro nos da una idea de cómo aumenta el número de funtores monádicos y diádicos a medida que aumenta el número de valores de verdad (si ya nos cuesta nom-

brar los 20 funtores monádicos o diádicos de la lógica bivalente, cuánto más los 19 710 de la trivalente, o de ella en adelante).

N.º de valores de verdad	2	3	4
n.º de funtores monádicos	$2^{2^1} = 4$	$3^{3^1} = 27$	$4^{4^1} = 256$
n.º de funtores diádicos	$2^{2^2} = 16$	$3^{3^2} = 19\,683$	$4^{4^2} = 4\,294\,967\,296$

Cuadro 9.1.— Número de funtores en lógicas polivalentes.
—*Fuente:* Elaboración propia.

Se desarrollaron varias lógicas de n-valores en los años treinta. Estas lógicas solían valorarse en el siguiente subconjunto de números racionales del intervalo $[0,1]$:

$$\begin{aligned} \mathrm{u}^n([0,1]) &= \left\{\frac{0}{n-1}, \frac{1}{n-1}, \frac{2}{n-1}, \ldots, \frac{n-1}{n-1}\right\} \\ &= \left\{0, \frac{1}{n-1}, \frac{2}{n-1}, \ldots, 1\right\} \\ &= T_n, \end{aligned}$$

pudiéndose interpretar tales valores como *grados de verdad*.[5]

La lógica de n-valores ($n \geq 2$) de Łukasiewicz, denotada L_n, tiene como primitivas:

$$\neg a \fallingdotseq 1 - a,$$
$$a \to b \fallingdotseq \min(1, 1 + b - a),$$

y los demás juntores se definen:

$$a \vee b \fallingdotseq (a \to b) \to b,$$
$$a \wedge b \fallingdotseq \neg(\neg a \vee \neg b),$$
$$a \leftrightarrow b \fallingdotseq (a \to b) \wedge (b \to a),$$

de donde:

$$a \vee b \fallingdotseq \max(a, b),$$
$$a \wedge b \fallingdotseq \min(a, b),$$
$$a \leftrightarrow b \fallingdotseq 1 - |a - b|\,.$$

[5] El subconjunto $\mathrm{u}^n([0,1])$ apareció con el nombre de *α-percentilado uniforme de cardinal n* en la tesis doctoral de quien escribe (*vid.* León Rojas [1] —definición 83 (pág. 120)—), en el ámbito del problema de la medición de la disimilitud entre dos subconjuntos de un retículo normado.

Enaria: implementación física

En cuanto a la implementación física de estas lógicas con más de tres valores de verdad, digamos de las arquitecturas de celdas con múltiples niveles[*] de ciertas memorias Flash[†] —por ejemplo, las StrataFlash[‡]—, que las memorias con cinco niveles por celda siguen en desarrollo, esto es, actualmente las memorias Flash trabajan como mucho con cuatro niveles por celda, y que, aunque varios esquemas de modulación de señales codifican muchos niveles, no es algo que se use para computación general. La razón es que mientras que representar físicamente una señal ternaria es sencillo (el voltaje puede ser positivo, negativo o nulo), hacer lo mismo con un mayor número de niveles es más complicado. Harían falta circuitos mucho más precisos, que se verían más afectados por el ruido.

[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/Multi-level_cell.
[†] *Vid. v. gr.* https://en.wikipedia.org/wiki/Flash_memory.
[‡] *Vid. v. gr.* https://en.wikipedia.org/wiki/StrataFlash.

§ 9.2 Lógicas infinitamente valoradas

Las lógicas de Łukasiewicz se presentan en la sucesión $L_2, L_3, \ldots, L_n, \ldots$, con límite L_∞. Por ésta se nota la lógica (infinitamente) valorada en el conjunto numerable T_∞ de todos los números racionales de $[0,1]$. La llamada *lógica estándar de* Łukasiewicz L_1 se valora (infinitamente) en $[0,1]$ (el 1 subíndice de L_1 es una abreviatura de $\aleph_1$, el cardinal del continuo en ZFC+HGC). Generalmente en la literatura, por *lógica infinitamente valorada* se entiende la valoración en $[0,1]$. Un resultado bien conocido es que para ninguna lógica infinitamente valorada existe un conjunto finito *completo* de primitivas[6]. Completitud del conjunto en el sentido de capacidad de generar toda la lógica; es decir, que al usar un conjunto finito de primitivas para definir una lógica infinitamente valorada, sólo obtendremos un subconjunto de todas las funciones lógicas.

La lógica estándar de Łukasiewicz L_1 es isomorfa a la teoría de conjuntos borrosos estándar en el mismo sentido que la lógica de juntores es isomorfa (como álgebra de Boole) a la teoría estándar de conjuntos. De hecho para cualquier lógica infinitamente valorada existe una teoría de conjuntos borrosos isomorfa a ella, obtenida con un conjunto particular de operadores borrosos. Así,como ejemplo de lógica valorada en todo $[0,1]$, tenemos la *lógica borrosa* (o, sinónimamente, *lógica difusa* [*fuzzy logic*])[7]. En la lógica borrosa: la negación de p se define como $\mu_{\neg p} = 1 - \mu_p$; la conjunción de p y q puede definirse de varias formas, a modo de ejemplo, utilizando el mínimo, $\mu_{p \wedge q} = \text{mín}(\mu_p, \mu_q)$, o utilizando el producto, $\mu_{p \wedge q} = \mu_p \cdot \mu_q$; la disyunción de p y q también puede definirse de varias formas, a modo de ejemplo, utilizando el máximo, $\mu_{p \vee q} = \text{máx}(\mu_p, \mu_q)$, o usando el principio de inclusión-

[6] *Cfr.* Klir y Yuan [139] (pág. 220).
[7] La lógica borrosa se ha mostrado como una herramienta muy útil en la toma de decisiones en ambientes de imprecisión, vaguedad e incertidumbre —*cfr. v. gr.* León Rojas [1] (capítulo 4)—, a veces, emparejada con la probabilidad bayesiana —*cfr. v. gr.* León Rojas [1] (capítulos 15–17)—.

exclusión, $\mu_{p\vee q} = \mu_p + \mu_q - \mu_p \cdot \mu_q$; la implicación $p \to q$ puede definirse también de varias formas, a modo de ejemplo, la implicación de ZADEH, $\mu_{p\to q} = \text{máx}(1-\mu_p, \mu_q)$, o la implicación de MAMDANI, $\mu_{p\to q} = \text{mín}(1, 1-\mu_p+\mu_q)$, o la implicación de GÖDEL, $\mu_{p\to q} = 1$ si $\mu_p \leq \mu_q$, y $\mu_{p\to q} = \mu_q$ si $\mu_p > \mu_q$.

Las reglas de inferencia de la lógica borrosa son una extensión de las de la lógica bivalente; por ejemplo, la inferencia Si p entonces q, donde p y q son proposiciones borrosas, se realiza evaluando el grado de verdad de p y determinando el grado de verdad de q en función de la implicación elegida.

La composición de reglas también se puede realizar de diferentes formas; a modo de ejemplo, como composición max-min o como composición max-product, así en el primer caso, para un conjunto de reglas de la forma R_i : Si p_i entonces q_i, el grado de verdad de la conclusión agregada q se obtiene como $\mu_q(y) = \text{máx}_i\left(\text{mín}(\mu_{p_i}(x), \mu_{q_i}(y))\right)$, mientras que con la composición max-product, el grado de verdad de la conclusión agregada q es $\mu_q(y) = \text{máx}_i\left(\mu_{p_i}(x) \cdot \mu_{q_i}(y)\right)$.

§ 9.3 Lógica cuántica

La unidad básica de información cuántica es el cúbit. Éstos pueden existir en un estado conocido como superposición en el que valen a la vez 0 y 1, lo que permite a cada cúbit en el ámbito de la computación cuántica realizar dos cálculos a la vez.

Un cúbit es una unidad básica de información cuántica, que se representa por un vector unitario (esto es, de módulo 1) en un espacio vectorial complejo de dos dimensiones. Matemáticamente, un cúbit se describe como:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

donde $|0\rangle$ y $|1\rangle$ (leídos *ket* cero y *ket* uno) son los estados base ortonormales, y α y β son números complejos que satisfacen $|\alpha|^2 + |\beta|^2 = 1$.

Un cúbit puede encontrarse en una combinación lineal de los estados $|0\rangle$ y $|1\rangle$ (esto es lo que se conoce como estado de superposición cuántica), siendo precisamente esto lo que permite que el cúbit represente simultáneamente ambos estados ket cero y ket uno.

En realidad, ket cero y ket uno son abreviaturas (notación de DIRAC) de los vectores

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

pudiendo representar un estado general del cúbit por el vector

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Las operaciones sobre cúbits se representan mediante matrices unitarias; por ejemplo, la compuerta HADAMARD (H), que crea una superposición equitativa de los estados $|0\rangle$ y $|1\rangle$:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Aplicando este operador al estado $|0\rangle$ obtenemos:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$

mostrando este resultado cómo un cúbit en el estado $|0\rangle$ se transforma en una superposición igual de $|0\rangle$ y $|1\rangle$.

Para saber más y para practicar, *vid. v. gr.*:

- https://plato.stanford.edu/entries/qt-quantcomp/;
- https://algassert.com/quirk;
- https://www.quantumplayground.net;
- David ARROYO GUARDEÑO. La amenaza cuántica que se avecina: preparativos para el 'Día Q'. *The Conversation*. 29.12.2025. https://doi.org/10.64628/AAO.547au5acc.

Sección B

Teoría de conjuntos

CAPÍTULO 10

Lógica de clases

«*Aus dem Paradies, das* CANTOR *uns geschaffen, soll uns niemand, vertreiben können* [Del paraiso, que CANTOR nos proporcionó, nadie nos podrá expulsar]».
(David HILBERT, *Über das Unendliche* (1925). En: *Grundlagen der Geometrie*, 7.ª ed., 1930 (pág. 274).

La lógica de clases permite identificar cada colección de entidades a partir de los parecidos y diferencias de éstas. El estudio de las similitudes, disimilitudes e interacciones entre colecciones, entidades o entre colecciones y entidades, la clasificación de las entidades o colecciones en nuevas colecciones, la ordenación de dichas colecciones o de las entidades, la tolerancia en dichas clasificaciones, la influencia de las preferencias de otras entidades o colecciones en tales clasificaciones u ordenaciones, forman parte de la lógica de relaciones. Estudiar qué pueden hacer (cómo se «comportan») las entidades en relación con otras entidades o colecciones, es un objetivo de la lógica de funciones. La caracterización del modo de estar relacionadas las entidades de una colección a partir de dichos comportamientos —determinados por funciones— está en la esencia de la lógica de estructuras.

§ 10.0 El lenguaje de la teoría de conjuntos

En nuestro grado de estudio, sepamos que el lenguaje de la teoría de clases/conjuntos $\mathcal{L}_{\text{TC}}$ es un lenguaje de primer orden con identidad° al que se le añade el signo de pertenencia $\in$.

§ 10.1 Desde la ingenuidad

Nuestro conocimiento está basado primariamente en nuestras observaciones. Observar el mundo para:

- identificar diferentes tipos de características (variables);
- generar descripciones de las entidades, esto es, para enumerar sus características individuales e identificar aquellas otras que no corresponden a cada entidad concreta;
- especificar diferencias entre entidades como diferencias entre características pertenecientes a la misma variable;
- describir las semejanzas entre entidades en relación a variables determinadas, y reconocer que dicha semejanza es relativa, dependiendo de las características que son comparadas;
- identificar las características esenciales compartidas entre dos o más entidades, identificando el tipo (variable) de las características, y
- reconocer una entidad perteneciente a una agrupación de entidades conforme a las características esenciales compartidas por todas las entidades de dicha agrupación;

observaciones que conducen al concepto de clase como una agrupación de entidades unidas alrededor de una o más características esenciales.

° *Vid. supra* § 5.6.0 (pág. 423 de esta edición).

Definición 10.0 (Definición primera de CANTOR).— En 1880, CANTOR define un conjunto como «toda colección, clase, agregado o totalidad M de objetos determinados y diferenciados por la intuición o el pensamiento (objetos que se denominan elementos de M)».

En 1901, RUSSELL se encontraba escribiendo su obra *Principia Mathematica*, cuando se dio cuenta que admitiendo como definición de conjuntos la anterior surgían paradojas en la teoría.

RUSSELL argumentaba de la siguiente manera. Distingamos dos clases de conjuntos, los conjuntos R, que son elementos de sí mismos, y los conjuntos no$-R$ que no son elementos de sí mismos. Sea $A = \{$todos los conjuntos no$-R\}$. Entonces, ¿es A un conjunto R o un conjunto no$-R$? Veamos. Si A es R entonces A es elemento de sí mismo, de donde, por definición de A, A es no$-R$ (contradicción). Por otro lado, si A es no$-R$, entonces A no es elemento de sí mismo, de donde, por definición de A, A es elemento de A y por tanto A es R (contradicción).

Esta es la conocida como *antinomia de* RUSSELL.

§ 10.2 Clases

La lógica clásica definía un *concepto* como la representación de una entidad sin que se afirmase ni negase nada de ella, llamando *comprensión* o *intensión* a la colección de notas o rasgos que lo integran y *extensión* a la colección de entidades que abarca.

Una proposición del tipo S es P, por ejemplo, «Todo número primo mayor que 2 es impar», precisamente es una proposición, porque en ella se afirma el predicado del sujeto (en este ejemplo, «ser impar» de «número primo mayor que 2») y porque se conoce o se puede colegir la verdad o falsedad de tal afirmación.

Al sujeto se le atribuye el predicado considerando dos aspectos:

0.°, como propiedad o característica de aquél, esto es, formando el predicado parte de la comprensión del sujeto (en este ejemplo, todo número primo mayor que 2 tiene la propiedad de ser impar, es decir, «número impar» forma parte de la comprensión del concepto «número primo mayor que 2»), y

1.°, como representante de la clase de entidades a la que pertenece el sujeto, esto es, formando el sujeto parte de la extensión del predicado (en este ejemplo, cualquier número primo mayor que 2 pertenece a la clase de los números impares, es decir, «número primo mayor que 2» forma parte de la extensión del concepto «número impar»).

Entendiéndose, pues, una clase, como una colección de entidades que coinciden en poseer alguna nota o rasgo común. A semejanza del concepto, la clase no existe en la realidad natural. Por ejemplo, la clase de las personas que enseñan es una entelequia, lo real son las personas que la forman.

Una misma entidad puede pertenecer a clases distintas, por ejemplo, una persona puede pertenecer a la clase de las personas que estudian y a la de las personas que saben divertirse.

§ 10.2.0 Clases destacadas

Según el número de entidades en la clase, distinguimos entre:

0. *clase vacía* (o, sinónimamente, clase *nula*) Λ (o, sinónimamente, $\emptyset$): clase a la que no pertenece ninguna entidad;
1. *clase unimembre* (o, sinónimamente, clase *singular* o *unitaria*): clase a la que sólo pertenece una entidad;
2. *clase bimembre* (o, sinónimamente, clase *binaria*): clase a la que sólo pertenecen dos entidades;
3. *clase trimembre* (o, sinónimamente, clase *ternaria*): clase a la que sólo pertenecen tres entidades;

⋮

n. clase *enemembre* (o, sinónimamente, clase *enaria*: clase a la que sólo pertenecen n entidades.

⋮

Ω. *clase universal* V: clase a la que pertenecen todas las entidades[1].

Ejemplo 289

Proporcionemos un ejemplo de clase vacía, otro de clase pentamembre y otro de clase universal.

Resolución.—

0. Clase vacía: «ningún hombre».
1. Clase pentamembre o quinaria: «Adela, Amelia, Angustias, Magdalena y Martirio» —ésta es una definición por extensión; su definición por comprensión es «las cinco hijas de Bernarda Alba»—.
2. Clase universal: «toda mujer». ■

§ 10.2.1 Principios de la lógica de clases

Tres son los principios generales que propuso y aplicó la lógica tradicional, que recogió la lógica de juntores[2] y que siguen formando parte de la lógica de clases. Son:

0.º, toda clase se identifica consigo misma (*principio de identidad*);

[1] Sobre el porqué de llamarla V, *vid. v. gr.* https://en.wikipedia.org/wiki/Von_Neumann_universe y https://en.wikipedia.org/wiki/Grothendieck_universe.

[2] *Vid. supra* definición 0.4.4 (pág. 39 de esta edición).

1.º, ninguna clase puede ser y no ser ella a la vez (*principio de la no contradicción*), y

2.º, entre una clase y su negación no existe ninguna clase intermedia (*principio del tercio excluso*).

§ 10.2.2 Todo conjunto es una clase

Entenderemos por tanto por clase cualquier colección de conjuntos que satisfaga un concepto —propiedad, predicado— ϕ dado.

Definición 10.1.— Sean $\phi x\vec{y}$ una fórmula de $\mathcal{L}_{\mathrm{TC}}$ donde x es un conjunto arbitrario e $\vec{y}(y_0, \ldots, y_k)$ un vector de conjuntos cualesquiera. Si $\vec{s}(s_0, \ldots, s_k)$ es un vector de conjuntos, entonces se define la *clase* de los x tales que $\phi x\vec{s}$ como la colección de todos los conjuntos x que satisfacen la propiedad $\phi x\vec{s}$; esta clase es designada por $\{x : \phi x\vec{s}\}$. Representaremos las clases por letras latinas mayúsculas.

Observación 10.2.0.— Para representar el concepto «los x tales que ϕ», Russell y Whitehead, en sus *Principia Mathematica* (1910), usaron el acento circunflejo $\hat{x}(\phi x)$, mientras que Church [112] propone la notación lambda[3], $\lambda x \phi x$.

Teorema 10.0
Todo conjunto es una clase.

Demostración.— En efecto, el conjunto a es la clase $A = \{x : x \in a\}$; es decir, en este caso, $k = 0$, $s_0 = a$, $\vec{s}(s_0, \ldots, s_k) = \vec{s}(s_0) = \vec{s}(a) = a$, y siendo $\phi xy \equiv x \in y$, entonces $\phi x\vec{s} \equiv \phi xa \equiv x \in a$. ∎

Observación 10.2.1.— En la demostración hemos diferenciado entre «a» —el conjunto— y «A» —la clase—, y así seguiremos haciendo siempre que sea necesario explicitar la distinción. Sin embargo, este teorema certifica que pueda notarse también con letras latinas mayúsculas a los conjuntos, precisamente por ser clases, como haremos a partir del subcapítulo § 10.3 (pág. 539 de esta edición) y es lo habitual en la literatura pedagógica tanto académica como popular.

§ 10.2.3 No toda clase es un conjunto

Una clase puede ser o no ser un conjunto.

Las clases que son conjuntos pueden caracterizarse de acuerdo al siguiente resultado.

Teorema 10.1
La clase $A = \{x : \phi x\vec{s}\}$ es un conjunto si, y sólo si, $(\exists y)(\forall x)(\phi x\vec{s} \leftrightarrow x \in y)$.

[3] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Lambda_calculus#Origin_of_the_lambda_symbol.

Observación 10.2.2.— El hecho de que toda subclase de un conjunto es un conjunto puede representarse por: si $(\exists y)(\forall x)(\phi x\vec{s} \rightarrow x \in y)$, entonces $A = \{x : \phi x\vec{s}\}$ es un conjunto.

Definición 10.2.— Una *clase propia* es una clase que no es un conjunto.

De hecho, para hacer afirmaciones para un conjunto arbitrario es deseable poder manejar el concepto de la cuantificación universal sobre conjuntos («para todo conjunto»), lo que lleva a preguntarnos si existe realmente como conjunto la colección de todos los conjuntos. Vemos en el teorema siguiente que no es así, de hecho, es una clase propia. Su demostración la haremos por reducción al absurdo usando el *axioma del par*[4] y el *axioma de regularidad*[5], por lo que la estudiaremos una vez estudiados dichos axiomas.

Teorema 10.2
La clase de todos los conjuntos, *la clase universal* —el universo de los conjuntos—, V, es una clase propia.

Demostración.— *Vid*. ejemplo 398 (pág. 769 de esta edición). ■

Observación 10.2.3.— También demostraremos que V no es un conjunto, una vez estudiado el teorema de Cantor, en el ejemplo 394 (pág. 740 de esta edición); en cualquier caso, estamos ante la paradoja de Cantor[6]).

En la demostración del siguiente teorema también usamos ambos axiomas, por lo que reza la misma recomendación sobre su estudio.

Teorema 10.3
La clase $R = \{x : x \notin x\}$ es precisamente la clase universal $V = \{x : x = x\}$ y, por lo tanto, que $R = \{x : x \notin x\}$ es una clase propia —de hecho, vimos cómo considerarla un conjunto lleva a contradicción (paradoja de Russell)—.

Demostración.— *Vid*. ejemplo 399 (pág. 770 de esta edición). ■

Observación 10.2.4.— Estamos en los márgenes de uno de los terrenos más complicados de las matemáticas, a saber, sus fundamentos. De las clases, lo único que diremos en este grado de estudio es que una clase determinada $\{x : \phi x\}$ será un conjunto cuando la teoría de conjuntos en la que trabajemos asegure que existe un conjunto que según dicha teoría sea igual a la clase dada (por ejemplo[7]: en ZFC, con dos nociones primitivas, conjunto y pertenencia, están prohibidas las

[4] *Cfr. infra* § 14.2.2 (pág. 759 de esta edición).
[5] *Cfr. infra* § 14.4.2 (pág. 769 de esta edición).
[6] *Cfr. infra* observación 14.10.2 (pág. 780 de esta edición).
[7] *Cfr. infra* § 14 (pág. 752 de esta edición).

clases; en NBG con tres nociones primitivas, conjuntos, clases y pertenencia, coexisten clases y conjuntos; etc.), y que cuando no ocurre esto, cuando $\forall y$ (conjunto) , $y \neq \{x : \phi x\}$, entonces $\{x : \phi x\}$ es una clase propia.

§ 10.2.4 Funtores de clases a enunciados (relaciones entre clases)

El lenguaje de la lógica de clases incluye un signo para la identidad o igualdad de clases, el cual se usa como igualador semiótico al abreviar una clase con un nombre, $A = \{x : \phi x\}$, pero también representa la relación de identidad o igualdad entre clases.

En este apartado presentamos seis funtores diádicos entre clases (relaciones): igualdad, no igualdad, inclusión, no inclusión, inclusión estricta y no inclusión estricta. En las propias definiciones es posible apreciar las correspondencias entre funtores lógicos y funtores de clases a clases.

Sean las clases $A = \{x : \phi x\}$ y $B = \{x : \psi x\}$.

0. *Relación de igualdad entre clases* $=$:

$$A = B \text{ si, y sólo si, } (\forall x)(\phi x \leftrightarrow \psi x),$$

1. *Relación de no igualdad entre clases* $\neq$:

$$\begin{aligned} A \neq B &\text{ si, y sólo si, } \neg(A = B) \\ &\text{ si, y sólo si, } (\exists x)(\phi x \nleftrightarrow \psi x) \\ &\text{ si, y sólo si, } (\exists x)(\phi x \veebar \psi x), \end{aligned}$$

esto es, el funtor no-igualdad corresponde al funtor lógico contravaledor.

2. *Relación de subclase o de inclusión entre clases*: $A \subseteq B$ se lee «A es subclase de B» o «(la clase) A está incluida en (la clase) B» y se define por

$$A \subseteq B \text{ si, y sólo si, } (\forall x)(\phi x \rightarrow \psi x),$$

esto es, el funtor subclase corresponde al funtor lógico implicador.

3. *Relación de no subclase o no inclusión entre clases* $\nsubseteq$ (o $\nsubseteqq$):

$$\begin{aligned} A \nsubseteq B &\text{ si, y sólo si, } \neg(A \subseteq B) \\ &\text{ si, y sólo si, } (\exists x)(\phi x \nrightarrow x) \\ &\text{ si, y sólo si, } (\exists x)(\phi x \wedge \neg\psi x), \end{aligned}$$

esto es, el funtor no-subclase corresponde al funtor lógico desimplicador.

4. *Relación de subclase propia o inclusión estricta entre clases*: $A \subset B$ —o $A \subsetneq B$, $A \varsubsetneq B$, $A \subsetneqq B$— se lee «A es subclase propia de B» o «(la clase) A está incluida estrictamente en (la clase) B» y se define por

$$\begin{aligned} A \subset B \text{ si, y sólo si, } & A \neq B \wedge A \subseteq B \\ \text{si, y sólo si, } & (\exists x)(\phi x \veebar \psi x) \wedge (\forall x)(\phi x \rightarrow \psi x). \end{aligned}$$

5. *Relación de no subclase propia o no inclusión estricta entre clases* $\not\subset$:

$$\begin{aligned} A \not\subset B \text{ si, y sólo si, } & \neg(A \subset B) \\ \text{si, y sólo si, } & \neg(A \neq B \wedge A \subseteq B) \\ \text{si, y sólo si, } & A = B \vee A \nsubseteq B \\ \text{si, y sólo si, } & (\forall x)(\phi x \leftrightarrow \psi x) \vee (\exists x)(\phi x \wedge \neg \psi x). \end{aligned}$$

6. *Relación de superclase*: $A \supseteq B$ se lee «A es superclase de B» y se define por

$$A \supseteq B \text{ si, y sólo si, } (\forall x)(\phi x \leftarrow \psi x),$$

esto es, el funtor de clase a enunciado superclase corresponde al funtor lógico replicador.

7. *Relación de no superclase*: $A \nsupseteq B$ (o $A \nsupseteqq B$) se lee «A no es superclase de B» y se define por

$$\begin{aligned} A \nsupseteq B \text{ si, y sólo si, } & \neg(A \supseteq B) \\ \text{si, y sólo si, } & (\exists x)(\phi x \nleftarrow x) \\ \text{si, y sólo si, } & (\exists x)(\neg \phi x \wedge \psi x), \end{aligned}$$

esto es, el funtor de clase a enunciado no-superclase corresponde al funtor lógico desreplicador.

8. *Relación de superclase propia*: $A \supset B$ —o $A \supsetneq B$, $A \varsupsetneq B$, $A \supsetneqq B$— se lee «A es superclase propia de B» y se define por

$$\begin{aligned} A \supset B \text{ si, y sólo si, } & A \neq B \wedge A \supseteq B \\ \text{si, y sólo si, } & (\exists x)(\phi x \veebar \psi x) \wedge (\forall x)(\phi x \leftarrow \psi x). \end{aligned}$$

9. *Relación de no superclase propia*: $A \not\supset B$ se lee «A no es superclase propia de B» y se define por

$$\begin{aligned} A \not\supset B \text{ si, y sólo si, } & \neg(A \supset B) \\ \text{si, y sólo si, } & \neg(A \neq B \wedge A \supseteq B) \\ \text{si, y sólo si, } & A = B \vee A \nsupseteq B \\ \text{si, y sólo si, } & (\forall x)(\phi x \leftrightarrow \psi x) \vee (\exists x)(\neg \phi x \wedge \psi x). \end{aligned}$$

En adelante y con frecuencia, relajaremos la notación en la forma siguiente:

- $x \in A$ designará ϕx;
- escribiremos $\{x \in A : \psi x\}$ o incluso $\{x \in A : x \in B\}$ en vez de $\{x : \phi x \wedge \psi x\}$.

Con esto, lo anterior se simplifica. Por ejemplo:

0. *Relación de igualdad entre clases* $=$:

$$A = B \text{ si, y sólo si, } (\forall x)(x \in A \leftrightarrow x \in B);$$

1. *Relación de no igualdad entre clases* $\neq$:

$$A \neq B \text{ si, y sólo si, } (\exists x)(x \in A \veebar x \in B).$$

2. *Relación de inclusión entre clases* $\subseteq$:

$$A \subseteq B \text{ si, y sólo si, } (\forall x)(x \in A \to x \in B).$$

3. *Relación de no inclusión entre clases* $\nsubseteq$ (o $\subsetneqq$):

$$A \nsubseteq B \text{ si, y sólo si, } (\exists x)(x \in A \wedge x \notin B).$$

4. *Relación de inclusión estricta entre clases* $\subset$ (o $\subsetneq$, $\subsetneq$, $\subsetneqq$):

$$A \subset B \text{ si, y sólo si, } (\exists x)(x \in A \veebar x \in B) \wedge (\forall x)(x \in A \to x \in B).$$

5. *Relación de no inclusión estricta entre clases* $\not\subset$:

$$A \not\subset B \text{ si, y sólo si, } (\forall x)(x \in A \leftrightarrow x \in B) \vee (\exists x)(x \in A \wedge x \notin B).$$

§ 10.2.5 Funtores entre clases (operaciones lógicas con clases)

Al igual que en el apartado anterior, consideremos las clases $A = \{x : \phi x\}$ y $B = \{x : \psi x\}$.

Al igual que en lógica de primer orden, los signos que representan las clases pueden componerse. En este punto destacamos cinco funtores entre clases (operaciones lógicas con clases):

0. *Funtor complemento* $^{\complement}$, que corresponde al funtor lógico $\neg$; la *clase complementaria*, negación o complemento de la clase A, esto es, la colección de entidades que no están en A, es la clase

$$A^{\complement} = \{x : \neg\phi x\},$$

que consta precisamente de las entidades que no están en la clase A, es decir,

$$x \in A^{\complement} \text{ si, y sólo si, } x \notin A.$$

1. *Funtor unión* $\cap$ (o *funtor suma*), que corresponde al funtor lógico $\vee$; la *clase unión* $A \cup B$ —o *clase reunión o suma* $A + B$— de las clases A y B, esto es, la colección de entidades que están en A, en B o en ambas, es la clase

$$\begin{aligned} A \cup B &= \{x : \phi x \vee \psi x\} \\ &= \{x : x \in A \vee x \in B\}. \end{aligned}$$

2. *Funtor intersección* $\cap$ (o *funtor producto*), que corresponde al funtor lógico $\wedge$; la *clase intersección* $A \cap B$ —o *clase producto* $A \cdot B$— de las clases A y B, esto es, la colección de entidades que están en A y en B, es la clase

$$\begin{aligned} A \cap B &= \{x : \phi x \wedge \psi x\} \\ &= \{x : x \in A \wedge x \in B\}. \end{aligned}$$

3. *Funtor diferencia* $-$ (o $\setminus$), que corresponde al funtor lógico $\nrightarrow$; la *clase diferencia* $A \setminus B$, esto es, la colección de entidades que están en A y no están en B, es la clase

$$\begin{aligned} A \setminus B &= \{x : \phi x \nrightarrow \psi x\} \\ &= \{x : \phi x \wedge \neg \psi x\} \\ &= \{x : x \in A \wedge x \notin B\}. \end{aligned}$$

4. *Funtor diferencia simétrica* Δ, que corresponde al funtor lógico $\veebar$; la *clase diferencia simétrica* $A \Delta B$ de las clases A y B, esto es, la colección de entidades que o bien están en A y no están en B o bien están en B y no están en A, es la clase

$$\begin{aligned} A \Delta B &= (A \setminus B) \cup (B \setminus A) \\ &= \{x : x \in A \wedge x \notin B\} \cup \{x : x \in B \wedge x \notin A\} \\ &= \{x : (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\} \\ &= \{x : x \in A \veebar x \in B\}. \end{aligned}$$

Observación 10.2.5.— Si bien al funtor diferencia de clases a clases le corresponde el funtor lógico $\nrightarrow$, también es cierto que es posible reescribir éste como una composición de funtores lógicos. En efecto, es admisible expresar $\phi x \nrightarrow \psi x$ como $\phi x \wedge \neg \psi x$ y esta última en notación prefijo (la habitual para funciones [funtores en este caso]), esto es, $(\wedge \circ \neg_1)(\phi x, \psi x)$ —aquí, primero actúa $\neg_1$ y después actúa $\wedge$, es decir, $(\wedge \circ \neg_1)(\phi x, \psi x) = \wedge(\phi x, \neg \psi x)$—.

Observación 10.2.6.— Los funtores lógicos negación conjunta $\downarrow$ (negación de $\vee$) e incompatibilidad $|$ (negación de $\wedge$) corresponden a dos composiciones de funtores de clases a clases, a saber, $\left(^{\complement} \circ \cup\right)$ y $\left(^{\complement} \circ \cap\right)$, respectivamente. Como vemos se trata de las correspondientes leyes de De Morgan.

- $(A \cup B)^{\complement} = \{x : (x \in A) \downarrow (x \in B)\} = A^{\complement} \cap B^{\complement}$; en efecto,

$$\begin{aligned}
(A \cup B)^{\complement} &= \{x : x \in A \vee x \in B\}^{\complement} \\
&= \{x : \neg(x \in A \vee x \in B)\} \\
&= \{x : (x \in A) \downarrow (x \in B)\} \\
&= \{x : x \notin A \wedge x \notin B\} \\
&= \{x : x \in A^{\complement} \wedge x \in B^{\complement}\} \\
&= A^{\complement} \cap B^{\complement}.
\end{aligned}$$

- $(A \cap B)^{\complement} = \{x : (x \in A) \mid (x \in B)\} = A^{\complement} \cup B^{\complement}$; en efecto,

$$\begin{aligned}
(A \cap B)^{\complement} &= \{x : x \in A \wedge x \in B\}^{\complement} \\
&= \{x : \neg(x \in A \wedge x \in B)\} \\
&= \{x : (x \in A) \mid (x \in B)\} \\
&= \{x : x \notin A \vee x \notin B\} \\
&= \{x : x \in A^{\complement} \vee x \in B^{\complement}\} \\
&= A^{\complement} \cup B^{\complement}.
\end{aligned}$$

§ 10.2.6 Producto cartesiano entre clases

Definición 10.3.— Sean A y B clases. El *producto cartesiano* de A por B, que designamos por $A \times B$, es la clase:

$$\{\langle x, y\rangle : x \in A \wedge x \in B\}\,. \tag{10.0}$$

Observación 10.2.7.— Si A y B son conjuntos, entonces $A \times B$ es un conjunto, pues $A \times B \subseteq 2^{2^{A \cup B}}$ y, por el *axioma del conjunto potencia*[8], la clase de las partes de un conjunto es un conjunto.

§ 10.2.7 Las clases en la lógica tradicional

Predicable, especie y género

La lógica tradicional llama:

- *predicable* al concepto universal susceptible de ser atribuido a una pluralidad de sujetos;

[8] *Cfr. infra*: *conjunto potencia* (§ 10.6 [pág. 542 de esta edición]), y *axioma del conjunto potencia* (§ 14.2.4 [pág. 760 de esta edición]).

- *especie* al predicable de una pluralidad de entidades que representa la esencia o naturaleza común de éstas, y
- *género* al predicable de una pluralidad de especies que representa los rasgos comunes de éstas.

En otras palabras, el género es la clase y la especie la subclase.

Género próximo de una especie es un género subordinante inmediato de la misma, mientras que *género remoto*, un género subordinante no inmediato.

Toda especie puede considerarse género.

Porfirio (232-305) llamaba *diferencia* a lo que permitía distinguir entre especies de un mismo género, concretamente al predicable de una especie que representa los rasgos no comunes con las demás especies coordinadas en el mismo género. Esta agregación de diferencia permite construir el árbol de Porfirio: se parte de un género, al que se agrega una diferencia, lo cual genera dos ramas, cada una de ellas especie del género anterior y, a su vez, nuevos géneros, a los cuales, a cada uno, se le agrega una diferencia y se repite el proceso. Esta construcción se ha basado en *división dicotómica* (o *bimembre*), cuya completitud, esto es, su exhaustividad, es aportada por cada diferencia y su negación.

Ejemplo 290

Partiendo de la clase (género) $\mathbb{Q}$ de los números racionales y de la subclase (especie) $\mathbb{N}$ de los números naturales, construyamos un pequeño árbol de Porfirio.

Resolución.— En efecto, pudiésemos hablar de la clase (género) $\mathbb{Q}$ de los números racionales y de la subclase (especie) $\mathbb{N}$ de los números naturales —hecho que concretaremos en el ejemplo 291 (pág. 538 de esta edición) tras definir la implicación entre clases—. Pues bien, la diferencia «ser múltiplo de 2» agregada al género número natural, permite diferenciar o dividir éste en dos especies, a saber, la de los números naturales pares y la de los números naturales impares. Estas, a su vez, son géneros. La diferencia «ser mayor que 10» agregada al género número natural par, permite dividir éste en dos especies, la de los números naturales pares mayores que 10 y la de los números naturales pares menores o iguales que 10. ■

Implicación entre clases

Observemos que Y es una subclase (especie) de la clase (género) X si, y sólo si, no existe ninguna entidad de Y que no sea de X. Solemos decir entonces que la clase Y se implica necesariamente en la clase X o, simplemente, que la clase Y *implica* la clase X —es necesario ser de X para ser de Y, esto es, no ser de X impide ser de Y—; denominamos *clase antecedente* a Y y *clase consecuente* a X. También decimos que Y está subordinada a X —ser de Y depende de ser de X, esto es, si no se es de X, no se es de Y—; así, denominamos *clase subordinada* a Y y *clase subordinante* a X.

Ejemplo 291

Relacionemos las clases $\mathbb{N}$ y $\mathbb{Q}$ mediante los conceptos definidos en el párrafo inmediatamente anterior.

Resolución.— Observemos que no existe un número natural que no sea racional. Precisamente por esto decimos que la clase $\mathbb{N}$ de los números naturales es una subclase (especie) de la clase $\mathbb{Q}$ de los números racionales (género). También decimos que la clase $\mathbb{N}$ se implica necesariamente en la clase $\mathbb{Q}$ o, simplemente, que la clase $\mathbb{N}$ implica la clase $\mathbb{Q}$ —es necesario que un número sea racional para que sea natural, esto es, no ser número racional impide ser número natural—; $\mathbb{N}$ es la clase antecedente y $\mathbb{Q}$ la clase consecuente. También decimos que $\mathbb{N}$ está subordinada a $\mathbb{Q}$ —ser número natural depende de ser número racional, esto es, si un número no es racional, no es natural—; $\mathbb{N}$ es la clase subordinada y $\mathbb{Q}$ es la clase subordinante. ■

Observación 10.2.8.— Como nos habremos ya dado cuenta al llegar estudiando aquí, la implicación en la lógica tradicional es precisamente la inclusión entre clases.

Clases y silogismos

Recordemos la primera figura, en sus cuatro modos válidos,

bArbArA	cElArEnt	dArII	fErIO
M es P	M no es P	M es P	M no es P
S es M	S es M	s es M	s es M
$\therefore$ S es P	$\therefore$ S no es P	$\therefore$ s es P	$\therefore$ s no es P

Pudiésemos leer estos modos en el lenguaje de la lógica de clases. Por ejemplo, en el primer modo, en la premisa mayor se establece que la clase M es subclase de P, en la premisa menor que la clase S es subclase de M, de donde se deduce que la clase S es subclase de P. Es decir, en realidad tenemos una vista de los cuatro modos de la primera figura con la inclusión de clases, la clase complementaria y la pertenencia a una clase:

bArbArA	cElArEnt	dArII	fErIO
$M \subseteq P$	$M \subseteq P^{\complement}$	$M \subseteq P$	$M \subseteq P^{\complement}$
$S \subseteq M$	$S \subseteq M$	$s \in M$	$s \in M$
$\therefore\ S \subseteq P$	$\therefore\ S \subseteq P^{\complement}$	$\therefore\ s \in P$	$\therefore\ s \notin P$

Quizás esta nueva lectura nos ayude a comprender mejor la fundamentación silogística.

Actividad 10.0

Expresemos el resto de figuras y modos válidos en función de la inclusión de clases, la clase complementaria y la pertenencia a una clase.

§ 10.3 Conjuntos

Estas notas no son el lugar para una mayor preocupación ni profundización en la teoría de clases. A partir de aquí, las únicas clases que consideraremos serán conjuntos. Trabajamos en ZFC[9], donde los diferentes axiomas aseguran que las operaciones básicas anteriores generan conjuntos a partir de conjuntos. En adelante, por lo general, también relajaremos la notación en la forma siguiente: dada una clase $A = \{x : \phi x\}$, $x \in A$ designará ϕx. Así, por ejemplo, para la unión, $A \cup B = \{x : x \in A \vee x \in B\}$.

Como vemos, para cualquier conjunto genérico usaremos letras latinas mayúsculas A, B, C, etc., si bien en presencia de clases pudiésemos notarlos con minúsculas; por ejemplo, al escribir sobre la antinomia de Russell es frecuente expresar la clase de los conjuntos no$-R$ como $\{x : x \notin x\}$. Asimismo, como también apreciamos, lo que pertenece a un conjunto se representa entre llaves $\{\}$.

Definición 10.4.— Dado un conjunto A, la expresión $a \in A$ designa el hecho de ser a un *elemento* de A. Leemos dicha expresión: «a pertenece al conjunto A» (o, sinónimamente, «a es elemento de A»).

Definición 10.5.— Es posible definir un conjunto de dos formas: I, por *extensión*, enumerando todos sus elementos, y II,por *comprensión*, definiendo todos sus elementos mediante las propiedades que los caracterizan.

Ejemplo 292

Discutamos la definición por extensión y por comprensión según sea un conjunto finito o infinito.

Resolución.— Si un conjunto es finito, pudiésemos definirlo enumerando todos sus elementos. No obstante, observamos que la cuestión de fondo es disponer de un procedimiento efectivo de enumeración de los elementos de un conjunto, sean aquéllos de la naturaleza que sean y su número finito para terminar la enumeración, aunque arbitrariamente grande.

Si el conjunto es infinito, es imposible, en principio, hacer eso. En este caso pudiésemos recurrir a la definición por comprensión: lo más sencillo sería indicar el esquema que siguen esos elementos —por ejemplo, es fácil que nos demos cuenta de que $A = \{2, 4, 6, 8, 10, 12, \dots\}$ es el conjunto de los

[9] *Cfr. infra* § 14 (pág. 752 de esta edición).

números pares—, no obstante el problema surge cuando quien lo lee no se da cuenta de la relación. Para evitar esto, resulta más conveniente escribir la propiedad que los caracteriza, así, $A = \{x : x \text{ es natural y par }\}$, o bien, $A = \{x \in \mathbb{N} : \exists y \in \mathbb{N}, x = 2y\}$, o bien, $A = \{(x \in \mathbb{N})(\exists y \in \mathbb{N})(x = 2y)\}$. ■

Conjuntos informantes

La propiedad que caracteriza un conjunto puede ser compleja. Es el caso, por ejemplo, de conjuntos construidos a partir de *conjuntos informantes*. En estos últimos, sus elementos son unidades de información u otros conjuntos informantes. A partir de ellos, pueden construirse otros conjuntos cuyos elementos van acompañados por sus propias «mochilas» de información —conjuntos informantes—; una posible representación sería como conjunto de conjuntos: $\{\{a_0, \{I_0\}\}, \{a_1, \{I_1\}\}, \ldots, \{a_n, \{I_n\}\}\}$, siendo $I_0, I_1, \ldots, I_n$ conjuntos informantes que, a su vez, pudiesen ser conjuntos no clásicos, por ejemplo, conjuntos borrosos*.

* *Vid. v. gr.* KLIR y YUAN [139].

§ 10.4 Igualdad e inclusión de conjuntos

Definición 10.6.— Decimos que dos conjuntos A y B son *iguales*, y notamos $A = B$, precisamente si contienen los mismos elementos.

Ni el *orden* ni la *repetición* de elementos importan para distinguir conjuntos: $\{2, 3\} = \{2, 2, 3\}$.

Definición 10.7.— Decimos que A es *subconjunto* de B y notamos $A \subseteq B$, precisamente si todo elemento de A es elemento de B. En signos lógico-matemáticos: $A \subseteq B \coloneqq \forall x(x \in A \rightarrow x \in B)$. La relación $A \subseteq B$ se lee «A está *incluido o es igual* a B».

Definición 10.8.— Si $A \subseteq B$ pero $A \neq B$, o sea, que al menos un elemento de B no es elemento de A, decimos que A es *subconjunto propio* de B, y notamos $A \subset B$ («A está *incluido* en B»)[10].

Teorema 10.4

$A \subset B \rightarrow A \subseteq B$.

Observación 10.4.0.— El recíproco no es cierto, por ejemplo, sea $A = \{\text{Juan}\}$, y $B = \{\text{máximos acertantes en la Lotería}\}$, y supongamos que se ha celebrado el sorteo y que Juan

[10] La notación que empleamos fue propuesta por HAUSDORFF. Es necesario advertir que en algunos textos se interpreta $\subseteq$ como «estar incluido» y $\subset$ como «estar incluido estrictamente» o «propiamente», y, sobre todo, que en otros, la interpretación de $\subset$ permite la igualdad.

$\in B$; mientras que no finalice el recuento, sólo es posible asegurar que $A \subseteq B$, pues no sabemos si Juan es el único acertante, luego no es aceptable decir que $A \subset B$.

Observación 10.4.1.— Sean $A = \{x : x \in \mathbb{N} \wedge x \leq 10\}$ y $B = \{1, 3, 5, 7\}$. Claramente, $B \subset A$, de donde $A \not\subset B$. Estos símbolos también suelen escribirse al revés —en realidad se trata de relaciones de orden y de sus inversas[11], $A \supset B$ (A incluye a B). ¡Ojo! con lo anterior: $B \subset A$ no es equivalente a $A \not\subset B$, pues, $B \subset A$ implica $A \not\subset B$, pero el recíproco no es cierto, por ejemplo, $A = \{1, 2, 3\} \not\subset B = \{4, 5, 6\}$ y tampoco, $B \not\subset A$.

Observación 10.4.2.— Las relaciones de inclusión, representadas por los símbolos $\subseteq$ y $\subset$, deben entenderse como totalmente distintas de la relación de pertenencia $\in$. Por ejemplo, $\{2\} \subseteq \{2, 3\}$, y también $\{2\} \subset \{2, 3\}$, pero no es cierto $\{2\} \in \{2, 3\}$, ni $\{2\} \in \{\{2, 3\}\}$, ni $\{2\} \subseteq \{\{2, 3\}\}$, aunque sí lo son las afirmaciones, $2 \in \{2, 3\}$, $\{2\} \in \{\{2\}, \{3\}\}$ y $\{\{2\}\} \subset \{\{2\}, \{3\}\}$. El conjunto vacío es subconjunto de cualquier conjunto A, pero en general no es elemento de A. Asímismo, reflexionemos sobre el hecho de ser $x \in A \leftrightarrow \{x\} \subseteq A$ una fórmula válida.

Definición 10.9 (*Redefinición de igualdad de conjuntos*).— Sean dos conjuntos A y B. Entonces:

$$A = B \leftrightharpoons (A \subseteq B) \wedge (B \subseteq A)$$

Teorema 10.5
Por esta redefinición, demostrar la igualdad de dos conjuntos, es equivalente a demostrar la doble inclusión.

Observación 10.4.3.— Notemos la analogía existente entre las dos siguientes equivalencias en los dos ámbitos:

$$A = B \leftrightarrow (A \subseteq B) \wedge (B \subseteq A)$$

$$A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$$

§ 10.5 Conjuntos vacío, universal y unitarios

Se postula la existencia del conjunto que no contiene ningún objeto, que se llama *conjunto vacío* y se nota $\emptyset$. Así por ejemplo, en la consideración de todas las personas, actualmente el conjunto de las personas con varias antenas incrustadas en el cráneo es el conjunto vacío, pues en la actualidad es imposible encontrar una persona con tales características.

Definición 10.10.— Definimos el *conjunto vacío* como aquél cuyos elementos satisfacen una fórmula insatisfactible, por ejemplo, como el conjunto de todos los objetos que son distintos de sí mismos,

[11] *Cfr. infra* § 11.26 (pág. 644 de esta edición).

esto es,

$$\emptyset \risingdotseq \{x : x \neq x\}.$$

Notemos que si Px significa «$x \neq x$», Px es una concreción de $\perp$, por lo que $\emptyset \risingdotseq \{x : \perp\}$, de donde la *estructura lógica del conjunto vacío* es $\perp$.

Por contra, dada una situación concreta (esto es, un marco determinado de referencia o de trabajo), definimos el *conjunto universal* y se nota $\mathcal{U}$ como el conjunto que contiene todos los objetos.

Definición 10.11.— El (conjunto) *universal* (o, sinónimamente, *referencial*) es aquél cuyos elementos satisfacen una fórmula válida, por ejemplo,

$$\mathcal{U} \risingdotseq \{x : x = x\}.$$

Notemos que si Px significa «$x = x$», Px es una concreción de $\top$, por lo que $\mathcal{U} \risingdotseq \{x : \top\}$, de donde la *estructura lógica del conjunto universal* es $\top$.

Definición 10.12.— Denominamos *conjunto unitario* (o, sinónimamente, *conjunto elemental* o *átomo*) a aquél que tiene un único elemento, por ejemplo $\{\emptyset\}$.

Ejemplo 293

¿Cómo pudiésemos representar computacionalmente el conjunto $Y = \{2, 3\}$ en el «mundo» $\mathcal{U} = \{0, 1, 2, 3\}$?

Resolución.— Por ejemplo, mediante la palabra binaria 0011, cuyos bits, leídos de izquierda a derecha, representan el conocimiento siguiente: el primer 0, que 0 no está en Y, el segundo 0, que 1 no está en Y, el primer 1, que 2 está en Y y el segundo 1, que 3 está en Y. ■

§ 10.6 Conjunto potencia

Definición 10.13.— Denominamos *conjunto potencia* (o, sinónimamente, *conjunto de partes*) al conjunto de todos los subconjuntos del universal U. Lo notamos por $2^{\mathcal{U}}$ (o, sinónimamente, por $\mathcal{P}(\mathcal{U})$).

Análogamente a disponer del conjunto universal que contiene a todos los objetos, tenemos, dado un conjunto, el conjunto de todos sus subconjuntos.

Definición 10.14.— Análogamente a la definición anterior, denominamos *conjunto potencia de un conjunto* X (o, sinónimamente, *conjunto de las partes de un conjunto* X), al conjunto de todos los subconjuntos de X. Lo notamos por 2^X (o, sinónimamente, por $\mathcal{P}(X)$).

Ejemplo 294

¿Cuál es el conjunto potencia del conjunto $X = \{x, y, z\}$?

Resolución.— Si $X = \{x, y, z\}$, entonces

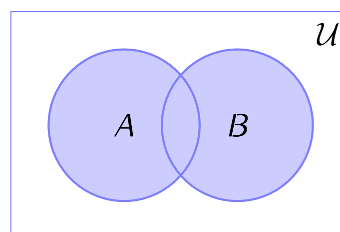
$$2^X = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}.$$ ■

§ 10.7 Unión e intersección de conjuntos

Los círculos que utilizamos para representar conjuntos son una evolución de los diagramas de Venn. Pudiésemos llamarlos *diagramas conjuntistas de* Venn. A diferencia de los círculos usados en lógica; en su uso con conjuntos, las áreas blancas designan áreas vacías y las áreas coloreadas designan áreas de las que no sabemos si están vacías o no, pero que de existir entidades en los conjuntos, aquéllas estarían en dichas áreas.

Definición 10.15.— El conjunto *unión* de los conjuntos A y B, notado $A \cup B$, es el conjunto de todos los objetos que son elementos de A, de B o de ambos, lo cual, expresado con signos lógico-matemáticos, es

$$A \cup B \leftrightharpoons \{x : x \in A \vee x \in B\}.$$



Notemos que si interpretamos Px como «x es elemento de A» y Qx como «x es elemento de B», entonces $A \cup B \leftrightharpoons \{x : Px \vee Qx\}$, por lo que la *estructura lógica de la unión* de dos conjuntos es

$$Px \vee Qx.$$

Teorema 10.6 (Propiedades de la unión respecto de la inclusión)

Se satisface $\forall X, Y \in \mathcal{P}(\mathcal{U})$:

0. $X \subseteq X \cup Y$;
1. $Y \subseteq X \cup Y$;
2. $X \subseteq Y \leftrightarrow X \cup Y = Y$.

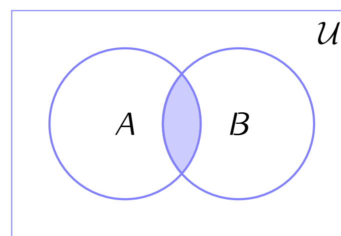
Teorema 10.7 (Propiedades de estructura de la unión de conjuntos)
Se satisface $\forall X, Y, Z \in \mathcal{P}(\mathcal{U})$:

0. $X \cup Y \subseteq \mathcal{U}$; ($\mathcal{P}(\mathcal{U})$ es parte estable para $\cup$)
1. $X \cup Y = Y \cup X$; (conmutativa de $\cup$)
2. $(X \cup Y) \cup Z = X \cup (Y \cup Z)$; (asociativa de $\cup$)
3. $X \cup \emptyset = X$; ($\emptyset$ es el elemento neutro de $\cup$ en $\mathcal{P}(\mathcal{U})$)
4. $X \neq \emptyset \rightarrow \neg\exists Y(Y \in \mathcal{P}(\mathcal{U}) \wedge X \cup Y = \emptyset)$; (salvo $\emptyset$, ningún $X \in \mathcal{P}(\mathcal{U})$ tiene simétrico)
5. $X \cup X = X$; (idempotencia de $\cup$)
6. $X \cup \mathcal{U} = \mathcal{U}$. ($\mathcal{U}$ es un elemento absorbente de $\cup$ en $\mathcal{P}(\mathcal{U})$)

Observación 10.7.0.— De las propiedades de estructura 0, 1, 2 y 3 de la unión se sigue que $(\mathcal{P}(\mathcal{U}); \cup)$ es un monoide conmutativo[12] (cuyo elemento neutro es $\emptyset$).

Definición 10.16.— El conjunto *intersección* de los conjuntos A y B, notado $A \cap B$, es el conjunto de todos los objetos que son elementos de A y de B, lo cual, expresado con signos lógico-matemáticos, es

$$A \cap B \coloneqq \{x : x \in A \wedge x \in B\}.$$



Notemos que si Px significa «x es elemento de A» y Qx significa «x es elemento de B», entonces $A \cap B \coloneqq \{x : Px \wedge Qx\}$, por lo que la *estructura lógica de la intersección* de dos conjuntos es

$$Px \wedge Qx.$$

Teorema 10.8 (Propiedades de la intersección respecto de la inclusión)
Se satisface $\forall X, Y \in \mathcal{P}(\mathcal{U})$:

0. $X \cap Y \subseteq X$;
1. $X \cap Y \subseteq Y$;
2. $X \subseteq Y \leftrightarrow X \cap Y = X$.

[12] *Cfr. infra* § 17.4 (pág. 842 de esta edición).

Teorema 10.9 (Propiedades de estructura de la intersección de conjuntos)
Se satisface $\forall X, Y, Z \in \mathcal{P}(\mathcal{U})$:

0. $X \cap Y \subseteq \mathcal{U}$; ($\mathcal{P}(\mathcal{U})$ es parte estable para $\cap$)
1. $X \cap Y = Y \cap X$; (conmutativa de $\cap$)
2. $(X \cap Y) \cap Z = X \cap (Y \cap Z)$; (asociativa de $\cap$)
3. $X \cap \mathcal{U} = X$; ($\mathcal{U}$ es el elemento neutro de $\cap$ en $\mathcal{P}(\mathcal{U})$)
4. $X \neq \mathcal{U} \to \neg\exists Y(Y \in \mathcal{P}(\mathcal{U}) \wedge X \cap Y = \mathcal{U})$; (salvo $\mathcal{U}$, ningún $X \in \mathcal{P}(\mathcal{U})$ tiene simétrico);
5. $X \cap X = X$; (idempotencia de $\cap$)
6. $X \cap \emptyset = \emptyset$. ($\emptyset$ es un elemento absorbente de $\cap$ en $\mathcal{P}(\mathcal{U})$)

Observación 10.7.1.— De las propiedades de estructura 0, 1, 2 y 3 de la intersección se sigue que $(\mathcal{P}(\mathcal{U}); \cap)$ es un monoide conmutativo[13] (cuyo elemento neutro es $\mathcal{U}$).

Teorema 10.10 (Propiedades de estructura de la unión conjuntamente con la intersección)
Se satisface $\forall X, Y, Z \in \mathcal{P}(\mathcal{U})$:

0. $X \cup (Y \cap X) = X$; (simplificativa de $\cup$ en $\cap$)
1. $X \cap (Y \cup X) = X$; (simplificativa de $\cap$ en $\cup$)
2. $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$; (distributiva de $\cup$ en $\cap$)
3. $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$. (distributiva de $\cap$ en $\cup$)

Observación 10.7.2.— En el teorema anterior sólo figuran las simplificativas y distributivas por la izquierda porque $\cap$ es conmutativa en $\mathcal{P}(\mathcal{U})$.

Observación 10.7.3.— De la observación 10.7.0 (pág. 544 de esta edición), de la observación 10.7.1 (pág. 545 de esta edición) y de la distributiva de $\cap$ en $\cup$, se sigue que $(\mathcal{P}(\mathcal{U}); \cup, \cap)$ es un semianillo conmutativo y unitario[14].

Observación 10.7.4.— Notemos que:

- no es posible describir un conjunto unitario como unión de conjuntos distintos de él y del conjunto vacío, aunque
- sí es posible describir un conjunto unitario como intersección de conjuntos distintos de él y del conjunto universal.

[13] *Cfr. infra* § 17.4 (pág. 842 de esta edición).
[14] *Cfr. infra* § 17.7 (pág. 899 de esta edición).

Ejemplo 295

Siendo $A = \{0\}$ y $B = \{1\}$, hallemos $2^A \cap 2^B$.

Resolución.— $2^A = 2^{\{0\}} = \{\emptyset, \{0\}\}$ y $2^B = 2^{\{1\}} = \{\emptyset, \{1\}\}$, por lo que $2^A \cap 2^B = \{\emptyset\}$. ■

Actividad 10.1

Demostremos los teoremas anteriores.

§ 10.8 Conjuntos disjuntos

Definición 10.17.— Decimos que A y B son *conjuntos disjuntos* (o, sinónimamente, *conjuntos incompatibles* o *conjuntos intolerantes entre sí*)[15], precisamente si no tienen elementos en común, esto es, si, y sólo si,

$$A \cap B = \emptyset.$$

Observemos que si Px significa «x es elemento de A» y Qx significa «x es elemento de B», entonces la *estructura lógica* de la afirmación $A \cap B = \emptyset$ es

$$P \wedge Q \leftrightarrow \bot, \tag{10.1}$$

esto es, lo contradictorio de la ocurrencia conjunta de P y Q, de aquí lo de llamarles conjuntos incompatibles o intolerantes entre sí.

Ejemplo 296

El desarrollo de una asignatura universitaria se organiza en dos grupos grandes de clase A y B, que son tales que ninguna persona de un grupo pertenece al otro grupo. Utilicemos la teoría de conjuntos para demostrar que no pueden existir personas que pertenezcan a la vez a un subgrupo del A y a un subgrupo del B, sean los subgrupos del tamaño que sean siempre que contengan como mínimo una persona.

[PEP 14.4.2023:2]. *Cfr.* Anzola y Caruncho [140]: problema 2.7 (pág. 32).

Resolución.— Designemos los grupos grandes de clase A y B por los conjuntos A y B, respectivamente. Estos conjuntos A y B son disjuntos porque los grupos grandes de clase A y B son tales que ninguna persona de un grupo pertenece al otro grupo. Sean $S_A \subseteq A$ y $S_B \subseteq B$, ambos no vacíos

---

[15] Volveremos a hablar de compatibilidad o tolerancia cuando estudiemos las relaciones reflexivas y simétricas (relaciones de similitud, compatibilidad o tolerancia) —*cfr. supra* § 11.24 (pág. 638 de esta edición)— en las que las clases de similitud generadas por la relación no tienen por qué ser disjuntas.

porque cualesquiera subgrupos de los grupos grandes de clase A y B contienen como mínimo una persona. Razonemos por reducción al absurdo. Si existe $x \in S_A \cap S_B$, entonces $x \in S_A$ y $x \in S_B$, de donde $x \in A$ y $x \in B$ [porque $S_A \subseteq A$ y $S_B \subseteq B$], pero de aquí se sigue que $A \cap B \neq \emptyset$, en contra de la hipótesis de que A y B son disjuntos. ■

En el caso de más de dos conjuntos, distinguimos entre conjuntos mutuamente disjuntos y conjuntos disjuntos dos a dos.

Definición 10.18.— Decimos que $A_0, A_1, \ldots, A_n$ son *conjuntos mutuamente disjuntos* si, y sólo si, $A_0 \cap A_1 \cap \cdots \cap A_n = \emptyset$.

Definición 10.19.— Decimos que $A_0, A_1, \ldots, A_n$ son *conjuntos disjuntos dos a dos* si, y sólo si, $(\forall i, j \in \{0, 1, \ldots, n\})\,(i \neq j \to X_i \cap X_j = \emptyset)$.

Teorema 10.11

Si $A_0, A_1, \ldots, A_n$ son conjuntos disjuntos dos a dos, entonces son conjuntos mutuamente disjuntos. El recíproco no es cierto.

Actividad 10.2

Demostremos este último teorema.

Sugerencia.— La primera parte, por reducción al absurdo; la segunda, encontrando un contraejemplo.

[Cubit 65], [Cubit 66].

Con miras a su resolución.— *Primera parte.*— [Cubit 65] De una colección de conjuntos, supongamos que fuesen disjuntos dos a dos ($\leftrightharpoons P$) y no mutuamente disjuntos ($\leftrightharpoons \neg Q$), esto último significase que existiría al menos un elemento común a todos ellos, este elemento estaría en particular en dos de ellos, por lo que estos dos no serían disjuntos y, por lo tanto, los conjuntos de la colección no serían disjuntos dos a dos ($\neg P$). He aquí la contradicción a la que hemos llegado, los conjuntos de la colección son a la vez disjuntos dos a dos y no lo son ($P \wedge \neg P$). Por lo tanto, por reducción al absurdo se tiene que si son disjuntos dos a dos, son mutuamente disjuntos ($P \to Q$).

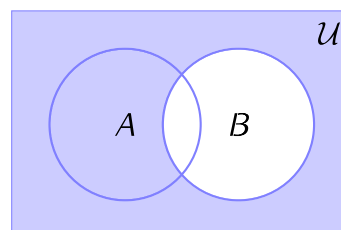
Segunda parte.— [Cubit 66] (El recíproco). Los conjuntos $\{0\}, \{1\}, \{0, 1\}$ son mutuamente disjuntos ($\{0\} \cap \{1\} \cap \{0, 1\} = \emptyset$), pero no son disjuntos dos a dos, pues si bien la intersección del primero y el segundo es vacía ($\{0\} \cap \{1\} = \emptyset$), tanto el primero como el segundo tienen intersección con el tercero ($\{0\} \cap \{0, 1\} = \{0\}$ y $\{1\} \cap \{0, 1\} = \{1\}$).

§ 10.9 Conjunto complementario

Dado un conjunto $A = \{x : Px\}$, definimos el conjunto cuyos elementos satisfacen la negación del predicado P y a tal nuevo conjunto lo denominamos complementario de A.

Definición 10.20.— Sea un conjunto B; el conjunto *complementario* de B, que notamos $B^{\complement}$ (o, sinónimamente, B', $\overline{B}$ o $\complement_{\mathcal{U}}B$), es el conjunto de todas las entidades que no están en B, esto es,

$$B^{\complement} \fallingdotseq \{x : x \notin B\}.$$



Notemos que si interpretamos Qx como «x es elemento de B», entonces $B^{\complement} \fallingdotseq \{x : \neg Qx\}$, por lo que la *estructura lógica del complementario de B* es

$$\neg Qx.$$

Teorema 10.12 (Propiedades de la complementación respecto de la inclusión)
Se satisface $\forall X, Y \in \mathcal{P}(\mathcal{U})$:

0. $X \subseteq Y \leftrightarrow X \cap Y^{\complement} = \emptyset$;
1. $X \subseteq Y \leftrightarrow X^{\complement} \cup Y = \mathcal{U}$;
2. $X \subseteq Y \leftrightarrow Y^{\complement} \subseteq X^{\complement}$.

Actividad 10.3

Demostremos el apartado 0 del teorema inmediatamente anterior.
Sugerencia.— [$\subseteq$] directa , [$\supseteq$] indirecta, por reducción al absurdo).

[Cubit 77].

Teorema 10.13 (Propiedades de estructura de la complementación)
Se satisface $\forall X \in \mathcal{P}(\mathcal{U})$:

0. $\emptyset^{\complement} = \mathcal{U}$; (complementación del vacío)
1. $\mathcal{U}^{\complement} = \emptyset$; (complementación del referencial)
2. $(X^{\complement})^{\complement} = X$. (involutiva[16] de $^{\complement}$)

[16] A veces llamada propiedad de *idempotencia* cuando la complementación es vista como una operación unitaria en $\mathcal{P}(\mathcal{U})$.

Teorema 10.14 (Propiedades de la complementación respecto de la unión o intersección)
Se satisface, para cualesquiera $X, X_0, X_1, \ldots, X_{n-1}, Y \in \mathcal{P}(\mathcal{U})$:

0. $X \cup X^{\complement} = \mathcal{U}$; (ley de complementación para $\cup$)
1. $X \cap X^{\complement} = \emptyset$; (ley de complementación para $\cap$)
2. $(X \cup Y)^{\complement} = X^{\complement} \cap Y^{\complement}$; (ley de De Morgan)
3. $(X \cap Y)^{\complement} = X^{\complement} \cup Y^{\complement}$; (ley de De Morgan)
4. $(X_0 \cup X_1 \cup \ldots \cup X_{n-1})^{\complement} = X_0^{\complement} \cap X_1^{\complement} \cap \ldots \cap X_{n-1}^{\complement}$; (ley de De Morgan generalizada)
5. $(X_0 \cap X_1 \cap \ldots \cap X_{n-1})^{\complement} = X_0^{\complement} \cup X_1^{\complement} \cup \ldots \cup X_{n-1}^{\complement}$. (ley de De Morgan generalizada)

Observación 10.9.0.— Démonos cuenta que si bien un conjunto y su complementario son disjuntos, del hecho de que dos conjuntos sean disjuntos no implica que sean complementarios entre sí.

Actividad 10.4

Demostremos los teoremas anteriores.

§ 10.10 El álgebra de Boole de los conjuntos

La cuaterna $(2^{\mathcal{U}}, \cap, \cup, {}^{\complement})$ tiene estructura de álgebra de Boole, que por su definición como retículo distributivo y complementado[17], siendo $\cap$, $\cup$ y ${}^{\complement}$ las operaciones correspondientes $\sqcap$, $\sqcup$ y $'$ de la definición, respectivamente— significa que $(2^{\mathcal{U}}, \cap, \cup, {}^{\complement})$

0. es un retículo, o sea, satisface las propiedades

   - conmutativas[18] de $\cup$ y $\cap$ en $\mathcal{P}(\mathcal{U})$, esto es, para cualesquiera X, Y de $\mathcal{P}(\mathcal{U})$ se satisface

$$X \cup Y = Y \cup X,$$
$$X \cap Y = Y \cap X,$$

   - asociativas[19] de $\cup$ y $\cap$ en $\mathcal{P}(\mathcal{U})$, esto es, para cualesquiera X, Y, Z de $\mathcal{P}(\mathcal{U})$ se satisface

$$(X \cup Y) \cup Z = X \cup (Y \cup Z),$$
$$(X \cap Y) \cap Z = X \cap (Y \cap Z),$$

[17] *Vid. supra* definición 3.17 (pág. 354 de esta edición).
[18] *Cfr. supra* teorema 10.7.1 (pág. 544 de esta edición) y teorema 10.9.1 (pág. 545 de esta edición), respectivamente.
[19] *Cfr. supra* teorema 10.7.2 (pág. 544 de esta edición) y teorema 10.9.2 (pág. 545 de esta edición), respectivamente.

- simplificativas[20], de $\cup$ en $\cap$ y de $\cap$ en $\cup$, esto es, para cualesquiera X, Y de $\mathcal{P}(\mathcal{U})$ se satisface

$$X \cup (Y \cap X) = X,$$
$$X \cap (Y \cup X) = X;$$

1. es un retículo distributivo, esto es, satisface además las propiedades

- distributivas[21], de $\cup$ en $\cap$ y de $\cap$ en $\cup$, esto es, para cualesquiera X, Y, Z de $\mathcal{P}(\mathcal{U})$ se satisface

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z),$$
$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z);$$

2. es un retículo distributivo y complementado, o sea, satisface además que

- es acotado, esto es, que existen los elementos neutros[22] de $\cup$ y $\cap$ en $\mathcal{P}(\mathcal{U})$, esto es, para todo X de $\mathcal{P}(\mathcal{U})$ se satisface

$$X \cup \emptyset = X,$$
$$X \cap \mathcal{U} = X,$$

- se satisfacen las leyes de complementación[23] para $\cup$ y $\cap$ en $\mathcal{P}(\mathcal{U})$, esto es, para todo X de $\mathcal{P}(\mathcal{U})$ se satisface

$$X \cup X^{\complement} = \mathcal{U},$$
$$X \cap X^{\complement} = \emptyset.$$

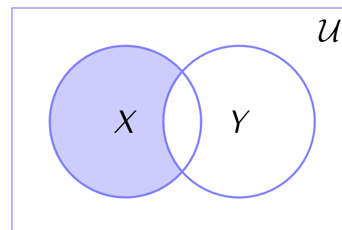
[20] *Cfr. supra* teorema 10.10.0 (pág. 545 de esta edición) y teorema 10.10.1 (pág. 545 de esta edición), respectivamente.
[21] *Cfr. supra* teorema 10.10.2 (pág. 545 de esta edición) y teorema 10.10.3 (pág. 545 de esta edición), respectivamente.
[22] *Cfr. supra* teorema 10.7.3 (pág. 544 de esta edición) y teorema 10.9.3 (pág. 545 de esta edición), respectivamente.
[23] *Cfr. supra* teorema 10.14.0 (pág. 549 de esta edición) y teorema 10.14.1 (pág. 549 de esta edición), respectivamente.

§ 10.11 Diferencia de conjuntos

Definición 10.21.— Sean dos conjuntos X y Y. El conjunto *complementario de Y en X*, notado $\complement_X Y$, es el conjunto de todos los elementos de X que no son elementos de Y, lo cual, expresado en lenguaje lógico-matemático, es

$$\complement_X Y \risingdotseq \{x : x \in X \land x \notin Y\}.$$

También denominamos a este conjunto, el *conjunto diferencia* de los conjuntos X y Y y lo notamos $X \setminus Y$ (o, sinónimamente, $X - Y$). Observemos que no es necesario que $Y \subseteq X$.



Observación 10.11.0.— La definición 10.20 (pág. 548 de esta edición) es el caso particular de la definición 10.21 (pág. 551 de esta edición) en el que $X = \mathcal{U}$.

Observemos que si interpretamos Px como «x es elemento de X» y Qx como «x es elemento de Y», entonces $\complement_X Y = X \setminus Y \risingdotseq \{x : Px \land \neg Qx\}$, por lo que la *estructura lógica del complementario de Y en X*, esto es, la *estructura lógica de la diferencia $X \setminus Y$*, es

$$Px \land \neg Qx. \tag{10.2}$$

> **Teorema 10.15** (Propiedad de la diferencia respecto de la inclusión)
> $(\forall X, Y \in \mathcal{P}(\mathcal{U}))(X \subseteq Y \leftrightarrow X \setminus Y = \emptyset)$.

Observación 10.11.1.— En su estructura lógica, este último teorema afirma que $Px \to Qx$ equivale lógicamente a $Px \land \neg Qx \leftrightarrow \bot$, esto es, a $\neg(Px \land \neg Qx)$, es decir, a $\neg Px \lor Qx$. Apreciamos que si hablásemos de intertraducción entre las álgebras de Boole de la lógica de juntores y de conjuntos, el implicador se traduciría, dependiendo del contexto, como la relación de inclusión o como el complementario de la diferencia.

> **Teorema 10.16** (Peculiaridades de la diferencia)
> $\forall X, Y, Z \in \mathcal{P}(\mathcal{U})$:
> 0. $X \setminus Y \neq Y \setminus X$; (no conmutativa)
> 1. $(X \setminus Y) \setminus Z \neq X \setminus (Y \setminus Z)$. (no asociativa)

Teorema 10.17 (Propiedades de estructura de la diferencia de conjuntos)
$\forall X, Y \in \mathcal{P}(\mathcal{U})$:
0. $X \setminus Y \subseteq \mathcal{U}$; ($\mathcal{P}(\mathcal{U})$ es parte estable para $\setminus$)
1. $X \setminus \emptyset = X$; ($\emptyset$ es neutro por la derecha)
2. $X \setminus X^{\complement} = X$;
3. $X \setminus X = \emptyset$; (todo conjunto es simétrico de sí mismo)
4. $\emptyset \setminus X = \emptyset$; ($\emptyset$ es absorbente por la izquierda)
5. $X \setminus \mathcal{U} = \emptyset$;
6. $\mathcal{U} \setminus X = X^{\complement}$;
7. $X^{\complement} \setminus X = X^{\complement}$.

Teorema 10.18 (Propiedades de interdefinición)
$\forall X, Y \in \mathcal{P}(\mathcal{U})$:
0. $X \setminus Y = X \cap Y^{\complement}$;
1. $X \setminus Y = X \setminus (X \cap Y)$.

Ejemplo 297

Siendo A, B y C tres conjuntos cualesquiera y designando por $\cup$, $\cap$, $\setminus$,$\subseteq$ y $=$, la unión, intersección, diferencia, inclusión e igualdad de conjuntos, respectivamente, entonces, utilizando teoría de conjuntos, demostremos que las tres afirmaciones $C \subseteq A \cup B$, $C \setminus A \subseteq B$ y $(C \setminus A) \cap (C \setminus B) = \emptyset$ son equivalentes.

[PEP 20.5.2022:2b], [EFO 20.5.2022:2].

Resolución.— I. Demostramos que $C \subseteq A \cup B \leftrightarrow C \setminus A \subseteq B$.

$\rightarrow$) Si $x \in C \setminus A$, entonces $x \in C$ y $x \notin A$ y como $C \subseteq A \cup B$, entonces $x \in B$ [al estar en C está en $A \cup B$, y al no estar en A, necesariamente está en B].

$\leftarrow$) Si $x \in C$, entonces $x \in C \cap A$ o $x \in C \cap A^{\complement}$ [porque $C = C \cap U = C \cap (A \cup A^{\complement}) = (C \cap A) \cup (C \cap A^{\complement})$, siendo U el universal].
Si $x \in C \cap A$, entonces $x \in A$ $(*)$ [por definición de intersección].
Si $x \in C \cap A^{\complement}$, entonces, $x \in B$ $(\dagger)$ [porque $C \cap A^{\complement} \subseteq B$ (por hipótesis) y por definición de subconjunto].
De $(*)$ y $(\dagger)$, $x \in A \cup B$.

II. Demostramos que $C \setminus A \subseteq B \leftrightarrow (C \setminus A) \cap (C \setminus B) = \emptyset$.

$\rightarrow$) Si $x \in C \setminus A$, entonces $x \in B$ [pues, por hipótesis, $C \setminus A \subseteq B$], esto es, $x \notin B^{\complement}$ [por definición de complementario], de donde $x \notin C \cap B^{\complement}$ [por definición de intersección], por

lo que $x \notin C \setminus B$ [por definición de $\setminus$]; en definitiva, ningún elemento de $x \in C \setminus A$ puede serlo de $x \in C \setminus B$, en otras palabras, $(C \setminus A) \cap (C \setminus B) = \emptyset$ [por definición de intersección].

←) Por una parte, si $x \in C \setminus A$, entonces $x \in C$ y $x \in A^{\complement}$ $(*)$ [porque $C \setminus A = C \cap A^{\complement}$ y por definición de intersección].
Por otra, si $x \in C \setminus A$, entonces $x \notin C \setminus B$ [porque $(C \setminus A) \cap (C \setminus B) = \emptyset$, por hipótesis], esto es, $x \notin C \cap B^{\complement}$ [por definición de $\setminus$], es decir, $x \in (C \cap B^{\complement})^{\complement}$ [por definición de complementario], de donde $x \in C^{\complement} \cup B$ [por ley de De Morgan e idempotencia $((B^{\complement})^{\complement} = B)$], o sea, $x \in C^{\complement}$ o $x \in B$ $(\dagger)$ [por definición de unión].
De $(*)$ y $(\dagger)$, $x \in (C \cap A^{\complement}) \cap (C^{\complement} \cup B)$, esto es, $x \in ((C \cap A^{\complement}) \cap C^{\complement}) \cup (C \cap A^{\complement}) \cap B)$ [distributiva de $\cap$ sobre $\cup$], es decir, $x \in \emptyset \cup (C \cap A^{\complement}) \cap B)$ [porque $C \cap C^{\complement} = \emptyset$] y, por tanto, $x \in B$ [por definición de intersección].

III. Por la propiedad transitiva de $\leftrightarrow$, se tiene que $C \subseteq A \cup B \leftrightarrow (C \setminus A) \cap (C \setminus B) = \emptyset$ y, por tanto, la equivalencia de las tres afirmaciones.

■

Ejemplo 298

Siendo A, B y C tres conjuntos y designando por $\cup$, $\setminus$, $\subseteq$ y $=$, la unión, diferencia, inclusión e igualdad de conjuntos, respectivamente, entonces, utilizando teoría de conjuntos, refutemos la afirmación: si $A = B \setminus C$, entonces $B = A \cup C$.

[EFO 17.1.2022:2a], [PEP 5.4.2022:2a], [EFE 19.1.2023:2a], [EFO 24.5.2023:2a].

Resolución.— Debemos refutar dicha afirmación, en otras palabras, demostrar que es falsa. Para ello, basta que proporcionemos un contraejemplo, esto es, un ejemplo para el que se satisfaga $A = B \setminus C$ y no se satisfaga $B = A \cup C$.

He aquí uno: $x \neq y$, $B = \{x\}$ y $C = \{y\}$.

En efecto, si $x \neq y$, $B = \{x\}$ y $C = \{y\}$, entonces $A = \{x\}$ [de la transitiva de la igualdad, por ser $A = B \setminus C$ y $B \setminus C = \{x\}$], de donde se sigue que $A \cup C = \{x\} \cup \{y\} = \{x, y\} \neq B$ [por ser $B = \{x\}$ y ser $x \neq y$]. ■

Observación 10.11.2.— Estudiando previamente qué efecto tiene en $A \cup C$ el que suceda $A = B \setminus C$, nos damos cuenta de que para refutar la afirmación basta que $C \nsubseteq B$. En efecto,

$$
\begin{aligned}
A = B \setminus C \to A \cup C &= (B \setminus C) \cup C && \text{[regla de sustitución]}\\
&= (B \cap C^{\complement}) \cup C && \text{[definición de diferencia de conjuntos]}\\
&= (B \cup C) \cap (C^{\complement} \cup C) && \text{[distributiva de } \cup \text{ en } \cap\text{]}\\
&= (B \cup C) \cap \mathcal{U} && \text{[ley de complementación]}
\end{aligned}
$$

$$= B \cup C, \qquad \text{[ley de identidad]}$$

esto es, si $A = B \setminus C$, entonces $B = A \cup C$ si, y sólo si, $B = B \cup C$, y esto último sucede si, y sólo si, $C \subseteq B$.

Ejemplo 299

Siendo A, B y C tres conjuntos y designando por $\cup$, $\setminus$, $\subseteq$ y $=$, la unión, diferencia, inclusión e igualdad de conjuntos, respectivamente, entonces, utilizando teoría de conjuntos, demostremos la afirmación: si $X \subseteq A \cup B$, entonces $X \setminus A \subseteq B$.

[EFO 17.1.2022:2b], [PEP 5.4.2022:2b], [EFE 19.1.2023:2b], [EFO 24.5.2023:2b]. *Cfr.* TRUSS [141]: ejercicio 5 (pág. 60).

Resolución.— Dicha afirmación es verdadera. En efecto, si $x \in X \setminus A$, entonces $x \in X$ y $x \notin A$ [por definición de diferencia de conjuntos] y como $X \subseteq A \cup B$, entonces $x \in B$ [como $x \in X$ y $X \subseteq A \cup B$, entonces $x \in A \cup B$, y como $x \notin A$, necesariamente $x \in B$]. ■

Observación 10.11.3.— De $X \subseteq A \cup B$ no se sigue $X \subseteq A \vee X \subseteq B$. Por ejemplo, $A = \{0, 1, 2\}$, $B = \{2, 3, 4\}$ y $X = \{1, 2, 3\}$.

Observación 10.11.4.— Otra vía de demostración: por una parte, como $(A \cup B) \setminus A = B \setminus (A \cap B)$ y $B \setminus (A \cap B) \subseteq B$, por transitiva de $\subseteq$, tenemos que $(A \cup B) \setminus A \subseteq B$; por otra, de $X \subseteq A \cup B$ [hipótesis] y $(A \cup B) \setminus A \subseteq B$ se sigue que $X \setminus A \subseteq B$ [esto es así porque dados tres conjuntos X, Y, Z, se satisface $X \subseteq Y \to X \cap Z \subseteq Y \cap Z$ (en el caso en estudio Y es $A \cup B$ y Z es $A^{\complement}$)].

Ejemplo 300

Siendo A, B y C tres conjuntos cualesquiera y designando por $\cup$, $\setminus$ y $=$, la unión, diferencia e igualdad de conjuntos, respectivamente, entonces, utilizando teoría de conjuntos, demostremos o refutemos la afirmación $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$.

[EFE 7.7.2021:2a].

Resolución.— Esta afirmación es falsa; refutémosla. Para ello, proporcionemos un contraejemplo. Sean $A = \{a, b, c\}$, $B = \{b\}$ y $C = \{c\}$, siendo a, b y c elementos distintos. Entonces, por una parte,

$$\begin{aligned} A \setminus (B \cup C) &= \{a, b, c\} \setminus (\{b\} \cup \{c\}) && \text{(por definición de } A, B \text{ y } C) \\ &= \{a, b, c\} \setminus \{b, c\} && \text{(por definición de } \cup) \\ &= \{a, b, c\} \cap \{b, c\}^{\complement} && \text{(por definición de } \setminus) \end{aligned}$$

$$= \{a\}, \qquad \text{(por definición de } \cap \text{ y } ^{\complement})$$

y, por la otra parte,

$$\begin{aligned}
(A \setminus B) \cup (A \setminus C) &= (\{a, b, c\} \setminus \{b\}) \cup (\{a, b, c\} \setminus \{c\}) && \text{(por definición de } A, B \text{ y } C)\\
&= \{a, c\} \cup \{a, b\} && \text{(por definición de } \setminus)\\
&= \{a, b, c\}, && \text{(por definición de } \cup)
\end{aligned}$$

de donde, como a, b y c son elementos distintos, hemos encontrado un ejemplo para el que $A \setminus (B \cup C) \neq (A \setminus B) \cup (A \setminus C)$, por lo que la afirmación de que $A \setminus (B \cup C)$ es igual a $(A \setminus B) \cup (A \setminus C)$ para tres conjuntos cualesquiera A, B y C, es falsa. ■

Observación 10.11.5.— Alternativamente a una demostración por contraejemplos pudiésemos haber hecho una demostración directa. Se tiene que

$$\begin{aligned}
A \setminus (B \cup C) &= A \cap (B \cup C)^{\complement} && \text{(por definición de } \setminus)\\
&= A \cap (B^{\complement} \cap C^{\complement}) && \text{(por ley de De Morgan)}\\
&= (A \cap A) \cap (B^{\complement} \cap C^{\complement}) && \text{(por asociativa e idempotencia de } \cap)\\
&= (A \cap B^{\complement}) \cap (A \cap C^{\complement}) && \text{(por asociativa y conmutativa de } \cap)\\
&= (A \setminus B) \cap (A \setminus C) && \text{(por definición de } \setminus)\\
&\subseteq (A \setminus B) \cup (A \setminus C) && \text{(por definiciones de } \cup \text{ y } \cap)
\end{aligned}$$

y por las propias definiciones de $\cup$ y $\cap$ y por un teorema conocido sabemos que la unión de dos conjuntos es igual a su intersección si, y sólo si, ambos conjuntos son el mismo (en este caso, si, y sólo si, $A \setminus B = A \setminus C$, de ahí que baste suponerlos distintos para que no ocurra —como en el contraejemplo: $A \setminus B = \{a, c\} \neq \{a, b\} = A \setminus C$—).

Ejemplo 301

Siendo A, B y C tres conjuntos cualesquiera y designando por $\cup$, $\setminus$ y $=$, la unión, diferencia e igualdad de conjuntos, respectivamente, entonces, utilizando teoría de conjuntos, demostremos o refutemos la afirmación $A \cup (B \setminus C) = (A \cup B) \setminus (A \cup C)$.

[EFE 7.7.2021:2b].

Resolución.— Esta afirmación es falsa. Proporcionemos un contraejemplo para su refutación. Sean $A = \{a\}$, $B = \{b\}$ y $C = \{c\}$, siendo a, b y c elementos distintos. Entonces, por una parte,

$$\begin{aligned}
A \cup (B \setminus C) &= \{a\} \cup (\{b\} \setminus \{c\}) && \text{(por definición de } A, B \text{ y } C)\\
&= \{a\} \cup \{b\} && \text{(por definición de } \setminus)\\
&= \{a, b\}, && \text{(por definición de } \cup)
\end{aligned}$$

y, por la otra parte,

$$
\begin{aligned}
(A \cup B) \setminus (A \cup C) &= (\{a\} \cup \{b\}) \setminus (\{a\} \cup \{c\}) && \text{(por definición de } A, B \text{ y } C\text{)}\\
&= \{a, b\} \setminus \{a, c\} && \text{(por definición de } \cup\text{)}\\
&= \{a, b\} \cap \{a, c\}^{\complement} && \text{(por definición de } \setminus\text{)}\\
&= \{b\}, && \text{(por definición de } \cap \text{ y } ^{\complement}\text{)}
\end{aligned}
$$

de donde, como a y b son elementos distintos, hemos encontrado un ejemplo para el que $A \cup (B \setminus C) \neq (A \cup B) \setminus (A \cup C)$, por lo que la afirmación de que $A \cup (B \setminus C)$ es igual a $(A \cup B) \setminus (A \cup C)$ para tres conjuntos cualesquiera A, B y C, es falsa. ■

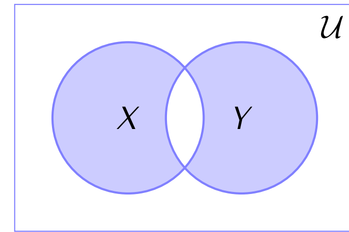
Actividad 10.5

Demostremos los teoremas anteriores.

§ 10.12 Diferencia simétrica

Definición 10.22.— Llamamos *diferencia simétrica* de los conjuntos X e Y, y notamos $X \Delta Y$, al conjunto $X \Delta Y \coloneqq (X \setminus Y) \cup (Y \setminus X)$, esto es,

$$X \Delta Y \coloneqq \{x \in X : x \notin Y\} \cup \{x \in Y : x \notin X\}$$



Notemos que si interpretamos Px como «x es elemento de X» y Qx como «x es elemento de Y», entonces $X \Delta Y \coloneqq \{x : Px \wedge \neg Qx\} \cup \{x : x : Qx \wedge \neg Px\}$, por lo que la *estructura lógica de la diferencia simétrica* $X \Delta Y$ es $(Px \wedge \neg Qx) \vee (Qx \wedge \neg Px)$, esto es,

$$Px \veebar Qx. \tag{10.3}$$

Observación 10.12.0.— Vista como operación, la diferencia simétrica se denomina *suma disyuntiva* y, en este caso, suele notarse con $\oplus$.

El siguiente teorema muestra algunas propiedades de Δ como operación en $\mathcal{P}(\mathcal{U})$.

Teorema 10.19 (Propiedades de estructura de la diferencia simétrica)
$\forall X, Y, Z \in \mathcal{P}(\mathcal{U})$:

0. $X \Delta Y \subseteq \mathcal{U}$; ($\mathcal{P}(\mathcal{U})$ es parte estable para Δ)
1. $\Delta Y = Y \Delta X$; (conmutativa);
2. $(X \Delta Y) \Delta Z = X \Delta (Y \Delta Z)$; (asociativa);
3. $X \Delta \emptyset = X$; ($\emptyset$ es el elemento neutro);
4. $X \Delta X = \emptyset$; (todo conjunto es su propio simétrico);
5. $X \cap (Y \Delta Z) = (X \cap Y) \Delta (X \cap Z)$. (distributiva de $\cap$ respecto de Δ).

Observación 10.12.1.— En el teorema anterior sólo figura la distributiva por la izquierda porque $\cap$ es conmutativa en $\mathcal{P}(\mathcal{U})$.

Observación 10.12.2.— Se satisface:

- $(\mathcal{P}(\mathcal{U}); \Delta)$ es un grupo conmutativo[24].
- $(\mathcal{P}(\mathcal{U}); \Delta, \cap)$ es un anillo conmutativo y unitario[25].

El siguiente teorema muestra algunas expresiones de Δ en función de $\cup$, $\cap$ y $^{\complement}$.

Teorema 10.20 (Propiedades de interdefinición)
$\forall X, Y \in \mathcal{P}(\mathcal{U})$:

0. $X \Delta Y = (X \cap Y^{\complement}) \cup (Y \cap X^{\complement})$;
1. $X \Delta Y = (X \cup Y) \cap (X \cap Y)^{\complement}$, esto es, $(X \cup Y) \setminus (X \cap Y)$;
2. $X \Delta Y = (X \cup Y) \cap (X^{\complement} \cup Y^{\complement})$.

Actividad 10.6

Demostremos el teorema 10.19 (pág. 557 de esta edición) y el teorema 10.20 (pág. 557 de esta edición).

Teorema 10.21 (Propiedades de inclusión)
$\forall X, X_0, X_1, Y, Y_0, Y_1 \in \mathcal{P}(\mathcal{U})$:

0. $(X_0 \cup X_1) \Delta (Y_0 \cup Y_1) \subseteq (X_0 \Delta Y_0) \cup (X_1 \Delta Y_1)$;
1. $X \Delta Y \subseteq X \rightarrow Y \subseteq X$.

[24] *Cfr. infra* § 17.5 (pág. 849 de esta edición).
[25] *Cfr. infra* § 17.8 (pág. 900 de esta edición).

Ejemplo 302

Siendo A y B dos conjuntos cualesquiera y designando por $\cup$, $\cap$, $\setminus$, $^{\complement}$, $\triangle$ y $=$, la unión, intersección, diferencia, complemento, diferencia simétrica e igualdad de conjuntos, respectivamente, entonces, utilizando teoría de conjuntos, demostremos la afirmación $(A \triangle B)^{\complement} = (A \cap B) \cup (A^{\complement} \cap B^{\complement})$.

[SEP 12.5.2022:2].

Resolución.— En efecto,

$$
\begin{aligned}
(A \triangle B)^{\complement} &= ((A \setminus B) \cup (B \setminus A))^{\complement} && \text{(por definición de } \triangle) \\
&= ((A \cap B^{\complement}) \cup (B \cap A^{\complement}))^{\complement} && \text{(por definición de } \setminus) \\
&= (A \cap B^{\complement})^{\complement} \cap (B \cap A^{\complement})^{\complement} && \text{(por ley de De Morgan)} \\
&= (A^{\complement} \cup (B^{\complement})^{\complement}) \cap (B^{\complement} \cup (A^{\complement})^{\complement}) && \text{(por ley de De Morgan)} \\
&= (A^{\complement} \cup B) \cap (B^{\complement} \cup A) && \text{(por ley de complementación)} \\
&= ((A^{\complement} \cup B) \cap B^{\complement}) \cup ((A^{\complement} \cup B) \cap A) && \text{(por distributiva de } \cap \text{ en } \cup) \\
&= ((A^{\complement} \cap B^{\complement}) \cup (B \cap B^{\complement})) \cup ((A^{\complement} \cap A) \cup (B \cap A)) && \text{(por distributiva de } \cap \text{ en } \cup) \\
&= ((A^{\complement} \cap B^{\complement}) \cup \emptyset) \cup (\emptyset \cup (B \cap A)) && \text{(por ley de complemento)} \\
&= (A^{\complement} \cap B^{\complement}) \cup (B \cap A) && \text{(por ley de identidad)} \\
&= (A^{\complement} \cap B^{\complement}) \cup (A \cap B) && \text{(por conmutativa de } \cap) \\
&= (A \cap B) \cup (A^{\complement} \cap B^{\complement}). && \text{(por conmutativa de } \cup) \quad \blacksquare
\end{aligned}
$$

Ejemplo 303

Siendo A, B y C tres conjuntos y designando por $\cap$, $\setminus$ y $\triangle$ la intersección, la diferencia y la diferencia simétrica de conjuntos, respectivamente, entonces, utilizando teoría de conjuntos,

0. refutemos la afirmación $A \triangle (B \cap C) = (A \triangle B) \cap (A \triangle C)$;
1. demostremos la afirmación $A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C)$;
2. utilicemos el apartado inmediatamente anterior para demostrar la afirmación $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

[Cubit 52], [EFO 4.6.2021:2]. *Cfr.* Truss [141]: ejercicio 9 (págs. 60 y 517).

Resolución.—

0. Para ello, proporcionemos un contraejemplo. Basta que $A = B$ y $A \cap C = \emptyset$; por ejemplo, sean $A = \{a\}$, $B = \{a\}$ y $C = \{c\}$, entonces, por una parte,

$$\begin{aligned}
A \triangle (B \cap C) &= \{a\} \triangle (\{a\} \cap \{c\}) && \text{(por defs. de } A, B \text{ y } C)\\
&= \{a\} \triangle \emptyset && \text{(por def. de } \cap)\\
&= (\{a\} \setminus \emptyset) \cup (\emptyset \setminus \{a\}) && \text{(por def. de } \triangle)\\
&= (\{a\} \cap \emptyset^{\complement}) \cup (\emptyset \cap \{a\}^{\complement}) && \text{(por def. de } \setminus)\\
&= (\{a\} \cap \mathcal{U}) \cup (\emptyset \cap \{a\}^{\complement}) && \text{(por defs. de } \emptyset \text{ y } \mathcal{U})\\
&= (\{a\} \cap \mathcal{U}) \cup \emptyset && \text{(por ley de dominación)}\\
&= \{a\} \cup \emptyset && \text{(por ley de identidad)}\\
&= \{a\}, && \text{(por ley de identidad)}
\end{aligned}$$

mientras que por la otra,

$$\begin{aligned}
(A \triangle B) \cap (A \triangle C) &= (\{a\} \triangle \{a\}) \cap (\{a\} \triangle \{c\}) && \text{(por defs. de } A, B \text{ y } C)\\
&= ((\{a\} \setminus \{a\}) \cup (\{a\} \setminus \{a\})) \cap \\
&\quad ((\{a\} \setminus \{c\}) \cup (\{c\} \setminus \{a\})) && \text{(por def. de } \triangle)\\
&= (\emptyset \cup \emptyset) \cap (\{a\} \cup \{c\}) && \text{(por def. de } \setminus)\\
&= \emptyset \cap (\{a\} \cup \{c\}) && \text{(por ley de identidad)}\\
&= \emptyset \cap \{a, c\} && \text{(por def. de } \cup)\\
&= \emptyset. && \text{(por ley de dominación)}
\end{aligned}$$

1. Dicha afirmación es verdadera; demostrémosla.

$$\begin{aligned}
A \cap (B \setminus C) &= A \cap B \cap C^{\complement} && \text{(por def. de } \setminus \text{ y asociativa de } \cap)\\
&= \emptyset \cup (A \cap B \cap C^{\complement}) && \text{(por ley de identidad)}\\
&= (B \cap \emptyset) \cup (A \cap B \cap C^{\complement}) && \text{(por ley de dominación)}\\
&= (B \cap (A \cap A^{\complement})) \cup (A \cap B \cap C^{\complement}) && \text{(por ley de complemento)}\\
&= ((A \cap B) \cap A^{\complement}) \cup ((A \cap B) \cap C^{\complement}) && \text{(por asociativa de } \cap)\\
&= (A \cap B) \cap (A^{\complement} \cup C^{\complement}) && \text{(por distributiva de } \cap \text{ respecto de } \cup)\\
&= (A \cap B) \cap (A \cap C)^{\complement} && \text{(por ley de De Morgan)}\\
&= (A \cap B) \setminus (A \cap C) && \text{(por definición de } \setminus)
\end{aligned}$$

2. Dicha afirmación es verdadera; demostrémosla.

$$A \cap (B \triangle C) = A \cap ((B \setminus C) \cup (C \setminus B)) \qquad \text{(por def. de } \triangle)$$

$$
\begin{aligned}
&= (A \cap (B \setminus C)) \cup (A \cap (C \setminus B)) && \text{(porque } \cap \text{ se distribuye en } \cup\text{)}\\
&= ((A \cap B) \setminus (A \cap C)) \cup ((A \cap C) \setminus (A \cap B)) && \text{(por apartado 1)}\\
&= (A \cap B) \triangle (A \cap C) && \text{(por def. de } \triangle\text{)} \quad \blacksquare
\end{aligned}
$$

Ejemplo 304

Siendo $^\complement$, $\cup$, $\cap$, $-$ y $\oplus$ las operaciones complementario, unión, intersección, diferencia y diferencia simétrica entre conjuntos, respectivamente, ¿cuál de las siguientes afirmaciones es verdadera?

a. Si $A \subseteq B$, entonces $A^\complement \cap B = \emptyset$.

b. $A^\complement - B^\complement = A - B$.

c. $A \oplus A = A$.

d. $(A - B)^\complement = A^\complement \cup B$.

[TT], [EFE 3.7.2024:2] (tipo test).

Resolución.— La opción a) es falsa; baste como contraejemplo tomar $A = \{0\}$ y $B = \{0, 1\}$ en el universo de los naturales, pues entonces $A = \{0\} \subseteq \{0, 1\} = B$, pero $A^\complement \cap B = \mathbb{Z}^+ \cap \{0, 1\} = \{1\} \neq \emptyset$.

La opción b) es falsa:

$$
\begin{aligned}
A^\complement - B^\complement &= A^\complement \cap (B^\complement)^\complement && \text{(por la definición de } -\text{)}\\
&= A^\complement \cap B && \text{(por la idempotencia de } ^\complement \text{ [ley de complementación])}\\
&= B \cap A^\complement && \text{(por la conmutativa de } \cap\text{)}\\
&= B - A. && \text{(por la definición de } -\text{)}
\end{aligned}
$$

La opción c) es falsa:

$$
\begin{aligned}
A \oplus A &= (A \cap A^\complement) \cup (A^\complement \cap A) && \text{(por la definición de } \oplus\text{)}\\
&= \emptyset \cup \emptyset && \text{(por las definiciones de } \cap \text{ y } ^\complement\text{)}\\
&= \emptyset. && \text{(por la ley de identidad)}
\end{aligned}
$$

La opción d) es verdadera:

$$
\begin{aligned}
(A - B)^\complement &= (A \cap B^\complement)^\complement && \text{(por la definición de } -\text{)}\\
&= A^\complement \cup (B^\complement)^\complement && \text{(por la ley de DE MORGAN)}\\
&= A^\complement \cup B. && \text{(por la idempotencia de } ^\complement \text{ [ley de complementación])}
\end{aligned}
$$

Solución.— Opción d. ■

Observación 10.12.3.— Recordemos que además de utilizar el álgebra de BOOLE de los conjuntos, tenemos múltiples posibilidades de demostración: contraejemplos, razonamiento diagramático, traducir a otro álgebra de BOOLE (lógica de juntores, circuitos combinacionales...), etc.

Ejemplo 305

Siendo $^{\complement}$, $\cup$, $\cap$, $-$ y $\triangle$ las operaciones complementario, unión, intersección, diferencia y diferencia simétrica entre conjuntos, respectivamente, ¿cuál de las siguientes afirmaciones es verdadera?

a. $A\triangle(B\cap C) = (A\triangle B)\cup(A\triangle C)$;

b. $A^{\complement}\cap B = A\triangle B^{\complement}$.

c. $A\triangle A^{\complement} = \emptyset$.

d. $(A\triangle B)^{\complement} = (A\cap B)\cup(A^{\complement}\cap B^{\complement})$

Sugerencia.— ¿Por qué no las traducimos al álgebra de BOOLE de la lógica de juntores?

[TT], [EFE 29.1.2025:2] (tipo test), [EFEC 29.1.2025:2] (tipo test).

Resolución.— Traducciones al álgebra de BOOLE de la lógica de juntores con sus tablas de verdad correspondientes son:

a. $p \veebar (q\wedge r) \leftrightarrow (p\veebar q)\vee(p\veebar r)$

p	q	r	$q\wedge r$	$p\veebar(q\wedge r)$	$p\veebar q$	$p\veebar r$	$(p\veebar q)\vee(p\veebar r)$	$p\veebar(q\wedge r)\boxed{\leftrightarrow}(p\veebar q)\vee(p\veebar r)$
1	1	1	1	0	0	0	0	1
1	1	0	0	1	0	1	1	1
1	0	1	0	1	1	0	1	1
1	0	0	0	1	1	1	1	1
0	1	1	1	1	1	1	1	1
0	1	0	0	0	1	0	1	0
0	0	1	0	0	0	1	1	0
0	0	0	0	0	0	0	0	1

b. $\neg p\wedge q \leftrightarrow p\veebar\neg q$.

p	q	$\neg p$	$\neg q$	$\neg p\wedge q$	$p\veebar\neg q$	$\neg p\wedge q\boxed{\leftrightarrow}p\veebar\neg q$
1	1	0	0	0	1	0
1	0	0	1	0	0	1
0	1	1	0	1	0	0
0	0	1	1	0	1	0

c. $p \veebar \neg p \leftrightarrow \bot$.

p	$\neg p$	$p \veebar \neg p$	$p \veebar \neg p \boxed{\leftrightarrow} \bot$
1	0	1	0
0	1	1	0

d. $\neg(p \veebar q) \leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$

p	q	$p \veebar q$	$\neg(p \veebar q)$	$p \wedge q$	$\neg p$	$\neg q$	$(\neg p \wedge \neg q)$	$(p \wedge q) \vee (\neg p \wedge \neg q)$	$\neg(p \veebar q) \boxed{\leftrightarrow} (p \wedge q) \vee (\neg p \wedge \neg q)$
1	1	0	1	1	0	0	0	1	1
1	0	1	0	0	0	1	0	0	1
0	1	1	0	0	1	0	0	0	1
0	0	0	1	0	1	1	1	1	1

Solución.— Opción d. ■

Actividad 10.7

El ejemplo 302 (pág. 558 de esta edición), ¿demuestra el teorema 10.20.2 (pág. 557 de esta edición)?

Actividad 10.8

Siendo ∩, \ y △ las operaciones intersección, diferencia y diferencia simétrica entre conjuntos, respectivamente, ¿cuál de las siguientes afirmaciones es verdadera?

a. $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$.

b. $A \setminus (B \setminus C) = (A \setminus B) \setminus C$.

c. $A \triangle A = A$.

d. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$.

§ 10.13 Traducción y traducción inversa

Para ambas, debemos tener en cuenta las secciones § 10.2.4 (pág. 532 de esta edición) y § 10.2.5 (pág. 534 de esta edición) y lo dicho en las definiciones anteriores acerca de las estructuras lógicas de las operaciones conjuntistas.

A modo de resumen, tenemos la siguiente relación entre el álgebra de Boole de la lógica de juntores $(\mathcal{F}_0; \wedge, \vee, \neg)$ y el álgebra de Boole de los conjuntos $(2^{\mathcal{U}}, \cap, \cup, ^{\complement})$:

$(\mathcal{F}_0; \wedge, \vee, \neg)$	$\bot$	id	$\neg$	$\vee$	$\wedge$	$\veebar$	$\rightarrow$	$\leftarrow$	$\not\rightarrow$	$\not\leftarrow$	$\leftrightarrow$	$\mid$	$\downarrow$	$\top$
$(2^{\mathcal{U}}, \cap, \cup, ^{\complement})$	$\emptyset$	id	$^{\complement}$	$\cup$	$\cap$	Δ	$\subseteq$ $\setminus^{\complement}$	$\supseteq$	$\not\subseteq$ $\setminus$	$\not\supseteq$	$=$	$\cap^{\complement}$	$\cup^{\complement}$	$\mathcal{U}$

observando también que $A \supseteq B = (B \setminus A)^{\complement}$ y que $A \not\supseteq B = B \setminus A$.

Por otra parte, a tenor de dichas estructuras lógicas de las operaciones conjuntistas, pensemos, por ejemplo, en el conjunto unión de los conjuntos A y B,

$$A \cup B = \{x : x \in A \vee x \in B\}.$$

Notemos que si interpretamos Px como «x es elemento de A» y Qx como «x es elemento de B», entonces la estructura lógica de la unión de dos conjuntos es $Px \vee Qx$.

Observemos también que entonces, la estructura lógica de su complementario es $\neg(Px \vee Qx) \equiv \neg Px \wedge \neg Qx$, de donde,

$$(A \cup B)^{\complement} = \{x : x \notin A \wedge x \notin B\},$$

lo cual, por involución del complementario, es

$$A \cup B = \{x : x \notin A \wedge x \notin B\}^{\complement},$$

definición equivalente de unión, que corresponde a la estructura lógica $\neg(\neg Px \wedge \neg Qx)$.

Dado que una de nuestras preocupaciones es la traducción de lenguaje lógico-matemático a nuestra lengua materna y la traducción inversa, desde nuestra lengua materna al lenguaje lógico-matemático, observemos finalmente que la expresión en español de esta definición alternativa del conjunto unión de los conjuntos A y B, aunque equivalente a la expresión en español dada al comienzo de la definición 10.15 (pág. 543 de esta edición), es menos natural que aquélla; en efecto, es suficiente compararlas:

Definición de $A \cup B$	Estructura lógica	Expresión en español
$\{x : x \in A \vee x \in B\}$	$Px \vee Qx$	Conjunto de todas las entidades que son elementos de A, de B o de ambos.
$\{x : x \notin A \wedge x \notin B\}^{\complement}$	$\neg(\neg Px \wedge \neg Qx)$	Conjunto de todas las entidades para las que es falso que ni sean elementos de A ni de B.

Por cierto, esto me recuerda el consejo estilístico y pragmático de reducir en lo posible las negaciones; por ejemplo, *Todo el mundo sabe que quien lo hizo mejor fue ella* es preferible a *Nadie ignora que no fue sino ella quien lo hizo mejor*, ¿verdad?

Actividad 10.9

Pensemos en traducciones alternativas para el resto de operaciones mencionadas: intersección, diferencia y diferencia simétrica.

Actividad 10.10

Representemos diagramáticamente con diagramas conjuntistas (no lógicos) de VENN la relación de inclusión según la traducción de la regla semántica de verdad de la implicación.

§ 10.14 Cardinal de un conjunto finito

Definición 10.23.— Dado un conjunto finito X, denominamos *cardinal* de X, y lo notaremos $|X|$ (o, sinónimamente, $card(X)$ o $\#(X)$), al número de elementos de X.

Ejemplo 306

Se satisface: $|\emptyset| = 0$, $|\{\emptyset\}| = 1$, $|\{\emptyset, \{\emptyset\}\}| = 2$.

Teorema 10.22 (Cardinal del complementario, de la unión y de la intersección)
$\forall X, Y \in \mathcal{P}(\mathcal{U})$:

0. si $Y \subseteq X$, entonces $|Y| = |X| - |X \setminus Y|$; (principio del complementario)
1. $|X \cup Y| = |X| + |Y| - |X \cap Y|$; (principio de inclusión-exclusión)
2. $|X \cap Y| \leq \text{mín}(|X|, |Y|) \leq \text{máx}(|X|, |Y|) \leq |X \cup Y|$.

Observación 10.14.0.— El principio del complementario aparecerá de nuevo como uno de los principios fundamentales de recuento al estudiar combinatoria enumerativa[26]. Una justificación rápida del principio de inclusión-exclusión es que al contar los elementos de X contamos una vez los de $X \cap Y$ y al contar los elementos de Y contamos otra vez los de $X \cap Y$, de aquí que haya que restar $|X \cap Y|$. También estudiaremos el principio de inclusión-exclusión como uno de los principios fundamentales de recuento[27], no sólo para dos conjuntos sino para un número finito de éstos. Como anticipo, fijémonos en qué establece para tres conjuntos: siendo X_0, X_1, X_2 tres conjuntos finitos, entonces se satisface

$$|X_0 \cup X_1 \cup X_2| = |X_0| + |X_1| + |X_2| - |X_0 \cap X_1| - |X_0 \cap X_2| - |X_1 \cap X_2| + |X_0 \cap X_1 \cap X_2|.$$

Ejemplo 307

De un total de n componentes software, determinemos el número de ellas sin fallos si hemos comprobado que la tercera parte presenta un fallo de tipo A, la tercera parte uno de tipo B, la tercera parte uno de tipo C, la quinta parte un par de ellos y la décima parte los tres fallos.

[Cubit 74], [SEL 4:2]. *Cfr.* Anzola y Caruncho [140]: ejercicio 7.55 (pág. 170).

Resolución.— Siendo S el conjunto de componentes software y X el conjunto de las que presentan un fallo de tipo X, para $X \in \{A, B, C\}$, pudiésemos interpretar la frase «la quinta parte un par de

[26] *Cfr. infra* teorema 19.21 (pág. 1143 de esta edición).
[27] *Cfr. infra* teorema 19.27 (pág. 1147 de esta edición).

ellos» de dos formas: I, $|A \cap B| = n/5$, $|A \cap C| = n/5$ y $|B \cap C| = n/5$, o bien, II, $|A \cap B| + |A \cap C| + |B \cap C| = n/5$. El número de componentes que presenta algún fallo es $|A \cup B \cup C|$, que por el principio de inclusión-exclusión es igual a $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$, esto es, según la primera interpretación, $n/3 + n/3 + n/3 - n/5 - n/5 - n/5 + n/10 = n(1 - 3/5 + 1/10) = n/2$, y según la segunda, $n/3 + n/3 + n/3 - n/5 + n/10 = n(1 - 1/5 + 1/10) = 9n/10$, por lo que, por el principio del complementario, el número de componentes que no presenta ningún fallo, $|(A \cup B \cup C)^{\complement}|$, es igual a $|S| - |A \cup B \cup C|$, que con la primera interpretación vale $n/2$ y con la segunda, $n/10$. ■

Teorema 10.23 (Cardinal del conjunto potencia)
Si $|X| = n$, entonces $|2^X| = 2^n$.

Demostración.— *Cfr. infra* ejemplo 411 (pág. 806 de esta edición). ■

Definición 10.24.— Una *métrica* en un conjunto es una función real no negativa —llamada también *función distancia* o simplemente *distancia*— $d : X \times X \longrightarrow [0, \infty)$, donde $[0, \infty)$ es el conjunto de números reales no negativos y tal que para cualesquiera $x, y, z \in X$, se satisface:

I. $d(x, y) = 0$ si, y sólo si, $x = y$; (identidad de los indistinguibles)

II. $d(x, y) = d(y, x)$; (simetría)

III. $d(x, z) \leq d(x, y) + d(y, z)$. (desigualdad triangular)

Ejemplo 308

La diferencia simétrica da una idea primaria de la «cercanía/lejanía» entre dos conjuntos. Definimos la *métrica diferencia simétrica*, dados dos conjuntos finitos X e Y, como el cardinal de su diferencia simétrica,

$$d_{\triangle}(X, Y) = |X \triangle Y|.$$

Demostremos que $d_{\triangle}$ es una métrica.

[CEOV 2020-2021 (p.h.e.c.)].

Resolución.— Sean tres conjuntos cualesquiera X, Y y Z.

I. ¿$d_{\triangle}(X, Y) = 0$ si, y sólo si, $X = Y$?, en otras palabras, ¿$|X \triangle Y| = 0$ si, y sólo si, $X = Y$?

En efecto,

$$\begin{aligned}
|X\triangle Y| = 0 &\leftrightarrow X\triangle Y = \emptyset && \text{(por definición de } \emptyset \text{ y cardinal)}\\
&\leftrightarrow (X\setminus Y)\cup(Y\setminus X) = \emptyset && \text{(por definición de } \triangle\text{)}\\
&\leftrightarrow X\setminus Y = \emptyset \text{ e } Y\setminus X = \emptyset && \text{(por definición de unión)}\\
&\leftrightarrow X\subseteq Y \text{ e } Y\subseteq X && \text{(por definición de } \setminus \text{ y } \subseteq\text{)}\\
&\leftrightarrow X = Y. && \text{(por definición de igualdad de conjuntos)}
\end{aligned}$$

II. ¿$d_\triangle(X,Y) = d(Y,X)$?, en otras palabras, ¿$|X\triangle Y| = |Y\triangle X|$?

Sí, por ser $X\triangle Y = (X\setminus Y)\cup(Y\setminus X) = (Y\setminus X)\cup(X\setminus Y) = Y\triangle X$ y tener, por tanto el mismo cardinal.

III. ¿$d_\triangle(X,Z) \leq d(X,Y) + d(Y,Z)$?, en otras palabras, ¿$|X\triangle Z| \leq |X\triangle Y| + |Y\triangle Z|$?

Demostremos primero que $X\triangle Z \subseteq (X\triangle Y)\cup(Y\triangle Z)$.

Si $x\in X\triangle Z$, entonces $x\in X\setminus Z$ o $x\in Z\setminus X$, esto es, sucede que $x\in X$ y $x\notin Z$ o que $x\in Z$ y $x\notin X$.

Por una parte, si $x\in X$ y $x\notin Z$, puede suceder que x esté en Y o no lo esté, pero en ambos casos es posible deducir lo pedido; en efecto:

0. si $x\in X$, $x\notin Z$ y $x\in Y$, entonces, de lo segundo y lo tercero, $x\in Y\triangle Z$ y, por tanto, $x\in(X\triangle Y)\cup(Y\triangle Z)$;

1. si $x\in X$, $x\notin Z$ y $x\notin Y$, entonces, de lo primero y lo tercero, $x\in X\triangle Y$ y, por tanto, $x\in(X\triangle Y)\cup(Y\triangle Z)$.

Por la otra, si $x\in Z$ y $x\notin X$, análogamente puede suceder que x esté en Y o no lo esté, y también en ambos casos es posible deducir lo pedido; en efecto:

0. si $x\in Z$, $x\notin X$ y $x\in Y$, entonces, de lo segundo y lo tercero, $x\in X\triangle Y$ y, por tanto, $x\in(X\triangle Y)\cup(Y\triangle Z)$;

1. si $x\in Z$, $x\notin X$ y $x\notin Y$, entonces, de lo primero y lo tercero, $x\in Y\triangle Z$ y, por tanto, $x\in(X\triangle Y)\cup(Y\triangle Z)$.

En definitiva, $X\triangle Z\subseteq(X\triangle Y)\cup(Y\triangle Z)$.

Por tanto, $|X\triangle Z|\leq|(X\triangle Y)\cup(Y\triangle Z)|$, de donde se deduce lo buscado. En efecto,

$$\begin{aligned}
|X\triangle Z| &\leq |(X\triangle Y)\cup(Y\triangle Z)|\\
&= |X\triangle Y| + |Y\triangle Z| - |(X\triangle Y)\cap(Y\triangle Z)|\\
&\leq |X\triangle Y| + |Y\triangle Z|.
\end{aligned}$$



Similaridad entre formas planas utilizando la diferencia simétrica

Ya hemos visto cómo para dos conjuntos es posible utilizar el cardinal de su diferencia simétrica como métrica para tener una medida de la distancia existente entre ellos. A modo de ejemplo, esto se particulariza al caso de de regiones poligonales en el plano utilizando el área de su diferencia simétrica como una métrica para así tener una medida de la similaridad existente entre ellas[*]. Los casos de regiones planas cualesquiera, superficies y volúmenes tridimensionales particulares o genéricos y regiones en espacios de más dimensiones quedan al albur de la inquietud y sagacidad de quien lee.

[*] *Cfr. v. gr.* Helmut ALT y Christian KNAUER, Matching shapes with respect to the symmetric difference, *Proceedings of the 15th European Workshop on Computational Geometry* (EWCG), Antibes-Juan-les-Pins, France, 195–197, 1999.

§ 10.15 Par ordenado y tupla ordenada

Definición 10.25.— Dados dos objetos a y b, definimos un nuevo objeto, el *par ordenado* $\langle a, b\rangle$, como el conjunto

$$\langle a, b\rangle = \{\{a\}, \{a, b\}\}$$

Decimos que a y b son la primera componente y la segunda componente, respectivamente, del par ordenado $\langle a, b\rangle$.

Teorema 10.24

La definición anterior de par ordenado satisface que

$$(\forall x)\,(\forall y)\,(\forall z)\,(\forall t)\,(\langle x, y\rangle = \langle z, t\rangle \leftrightarrow x = z \land y = t) \tag{10.4}$$

Observación 10.15.0.— KURATOWSKI definió par ordenado, en 1921, como la clase $\{\{x\}, \{x, y\}\}$, de manera que todo par ordenado es un conjunto no vacío que posee, a lo sumo, dos elementos[28]. HAUSDORFF lo definió en 1914 como $\{\{x, 1\}, \{y, 2\}\}$ y WIENER lo definió, también en 1914, como $\{\{x\}, \{y, \emptyset\}\}$[29].

La noción de *tupla*[30] generaliza el concepto de par ordenado (una *tupla diádica*). Si bien debemos tener cuidado al extender la definición, ya que, por ejemplo,

$$\langle\langle a, b\rangle, c\rangle \neq \langle a, \langle b, c\rangle\rangle; \tag{10.5}$$

[28] *Cfr.* ALONSO JIMÉNEZ, BORREGO DÍAZ, PÉREZ JIMÉNEZ y RUIZ REINA [142] (pág. 21).
[29] *Cfr.* BADESA, JANÉ y JANSANA [143] (pág. 43).
[30] *Cfr. supra* § 2 (pág. lxxviii de esta edición).

en efecto,

$$\langle\langle a,b\rangle,c\rangle = \langle\{\{a\},\{a,b\}\},c\rangle = \{\{\{\{a\},\{a,b\}\}\},\{\{\{a\},\{a,b\}\},c\}\}$$
$$\langle a,\langle b,c\rangle\rangle = \langle a,\{\{b\},\{b,c\}\}\rangle = \{\{a\},\{a,\{\{b\},\{b,c\}\}\}\}$$

Considerando entonces que debemos decidir extender la definición según qué alternativa, definimos la *tupla triádica* (o, sinónimamente, *terna ordenada*) como

$$\langle x_0, x_1, x_2\rangle = \langle\langle x_0, x_1\rangle, x_2\rangle\,, \tag{10.6}$$

la *tupla tetrádica* (o, sinónimamente, *cuaterna ordenada*) como

$$\langle x_0, x_1, x_2, x_3\rangle = \langle\langle x_0, x_1, x_2\rangle, x_3\rangle\,, \tag{10.7}$$

y, en general, siendo $n \in \mathbb{N} \wedge 2 \leq n$, la *tupla enádica* como

$$\langle x_0, x_1, \ldots, x_{n-1}\rangle = \langle\langle x_0, x_1, \ldots, x_{n-2}\rangle, x_{n-1}\rangle\,, \tag{10.8}$$

si bien hemos leído textos en los que se usan nombres más musicales, pero quizás también más plásticos, como cuarteto o cuarteta, quinteto y sexteto[31].

§ 10.16 Producto cartesiano

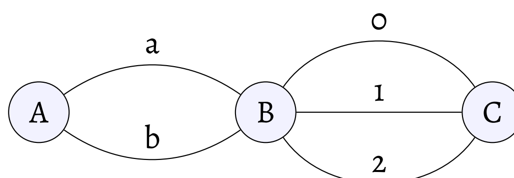


Figura 10.0.— Red de caminos entre tres ciudades.

Imaginemos tres ciudades A, B y C, conectadas las dos primeras por dos caminos, digamos a y b, y las dos segundas por tres, sean éstos 0, 1 y 2. Seguro que estamos de acuerdo en que hay un total de seis caminos, todas las posibles disposiciones de emparejamientos: $\langle a,0\rangle$, $\langle a,1\rangle$, $\langle a,2\rangle$, $\langle b,0\rangle$, $\langle b,1\rangle$, $\langle b,2\rangle$. Si llamamos a los conjuntos de los caminos entre A y B y entre B y C, $C_{AB} = \{a,b\}$ y $C_{BC} = \{0,1,2\}$, respectivamente, estos seis caminos son precisamente los elementos de un nuevo conjunto de caminos: el producto cartesiano $C_{AB} \times C_{BC}$. El estudio de las redes —como esta de caminos con tres nodos y cinco aristas—, de las que algo hemos escrito en estas notas[32] es parte de la rama de la matemática conocida como *topología*[33], el lenguaje del espacio.

[31] En español, *terna*, *trío* o *tripleta* se refiere a un conjunto de tres entidades, y, por otro lado, *dupla* no considera el orden sino el propósito, y *tripla*, *cuádrupla*, etc., aportarían un significado numeral multiplicativo que no vendría al caso.
[32] *Cfr. supra* § 10 (pág. ci de esta edición).
[33] *Vid. v. gr.* https://en.wikipedia.org/wiki/Topology.

Definición 10.26.— Sean A y B dos conjuntos. Llamamos *producto cartesiano* de A y B, y notamos $A \times B$, al conjunto de pares ordenados

$$A \times B \leftrightharpoons \{\langle x, y\rangle : x \in A \wedge y \in B\}\,.$$

Para más de dos conjuntos, por ejemplo, dados los conjuntos $A_0, A_1, \ldots, A_n$, tenemos que

$$A_0 \times A_1 \times \ldots \times A_n \leftrightharpoons \{\langle x_0, x_1, \ldots, x_n\rangle : x_0 \in A_0 \wedge x_1 \in A_1 \wedge \ldots \wedge x_n \in A_n\}\,.$$

Dos peculiaridades del producto cartesiano:

- *No es conmutativo*, ya que $\{\{x\}, \{x, y\}\} = \langle x, y\rangle \neq \langle y, x\rangle = \{\{y\}, \{y, x\}\}$.
- *No es asociativo* —*cfr.* (10.5) (pág. 567 de esta edición)—.

En el siguiente teorema destacamos algunas propiedades.

Teorema 10.25 (Algunas propiedades del producto cartesiano)
$\forall A, B, C$, conjuntos:
0. $A \times \emptyset = \emptyset \times A = \emptyset$; ($\emptyset$ es absorbente para $\times$)
1. $A \times B = \emptyset \leftrightarrow A = \emptyset \vee B = \emptyset$;
2. $A \times B \neq \emptyset \wedge A \times B = B \times A \rightarrow A = B$;
3. $A \times (B \cup C) = (A \times B) \cup (A \times C)$; ($\times$ se distribuye en $\cup$)
4. $A \times (B \cap C) = (A \times B) \cap (A \times C)$; ($\times$ se distribuye en $\cap$)
5. $\times$ es distributivo en $\setminus$: $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$; ($\times$ se distribuye en $\setminus$)
6. $(\forall m, n \in \mathbb{N})\,(|A| = m \wedge |B| = n \rightarrow |A \times B| = m \cdot n)$.

Hemos comenzado este subcapítulo con una representación del producto cartesiano como una red, para otras posibles representaciones, *vid. infra* § 11.1 (pág. 595 de esta edición).

Más allá de la tercera dimensión

Again, was I not taught by my Lord that as in a Line there are two *bounding points, and in a Square there are* four *bounding Lines, so in a Cube there must be* six *bounding Squares? ...And consequently does it not of necessity follow that the more divine offspring of the divine Cube in the land of Four dimensions, must have* 8 *bounding Cubes* [Además, ¿no fui instruido por mi Señor en que, así como en una Línea hay *dos* puntos delimitadores y en un Cuadrado hay *cuatro* Líneas delimitadoras, en un Cubo debe haber *seis* Cuadrados delimitadores? [...] Y, por consiguiente, ¿no se deduce necesariamente que el descendiente más divino del Cubo divino debe tener en la tierra de las Cuatro dimensiones 8 Cubos delimitadores?

(Edwin Abbott Abbott, *Flatland [Planilandia]*).

En efecto, ésta es una novela (una sátira matemática) que encuentra su hueco aquí, junto al producto cartesiano de conjuntos, *Planilandia*, de Edwin Abbott ABBOTT (https://archive.org/details/abbott-planilandia/mode/2up) (la original (1884), http://www.gutenberg.org/ebooks/201, y una película (de animación, en inglés), *Flatland: The Film* (2007), de Ladd EHLINGER, https://www.youtube.com/watch?v=avMX-Zft7K4.

§ 10.17 Propuesta de más actividades

Actividad 10.11

Elaboremos una tabla en la que recojamos la analogía entre juntores y operaciones de conjuntos.

Actividad 10.12

Sean A y B dos conjuntos no necesariamente disjuntos. Construyamos a partir de ellos dos conjuntos disjuntos A' y B'.

Actividad 10.13

Proporcionemos un ejemplo de tres conjuntos A, B y C tales que $A \in B$, $B \in C$ y $A \notin C$.

Actividad 10.14

Sean $A \neq \emptyset$ y $A_1, A_2, A_3 \subseteq A$, tales que $A_1 \subseteq A_2$, $A_2 \subseteq A_3$ y $A_3 \subseteq A_1$. Demostremos que $A_1 = A_2 = A_3$.

Actividad 10.15

Sean A y B dos conjuntos cualesquiera. Demostremos que: $A \subseteq B^c \leftrightarrow A \cap B = \emptyset \leftrightarrow A \setminus B = A \leftrightarrow A \cup B^c = B^c$.

Actividad 10.16

Dados dos conjuntos X e Y, ¿$2^{X \setminus Y} = 2^X \setminus 2^Y$?

Sugerencia.— Tras una reflexión, la intuición nos lleva a que una inclusión es verdadera pero la otra no; pudiésemos, pues, estudiar por doble inclusión la igualdad propuesta.

[Cubit 75].

Actividad 10.17

Sean A y B conjuntos y 2^A y 2^B sus conjuntos potencia. ¿Es cierto que $2^A \cup 2^B = 2^{A\cup B}$?

[Cubit 63], [SEL 4:1]. *Cfr.* Anzola y Caruncho [140]: ejercicio 2.30 (pág. 45).

Actividad 10.18

Demostremos que dados dos conjuntos A y B, si $A \cap B = \emptyset$, entonces $2^A \cap 2^B = \{\emptyset\}$. *Sugerencia.*— Por reducción al absurdo.

[Cubit 76].

Actividad 10.19

En una biblioteca hay más libros que revistas, más revistas españolas que libros científicos, más revistas no españolas científicas que libros no españoles no científicos. Demostremos que hay menos revistas no españolas no científicas que libros españoles no científicos.

[SEL 4:3]. *Cfr.* Anzola y Caruncho [140]: ejercicio 7.58 (pág. 173).

Actividad 10.20

¿Cuántos números de $\mathbb{Z}^+$, menores que 235, no son divisibles ni por 2 ni por 3 ni por 5?

[Cubit 78]. *Cfr.* Anzola y Caruncho [140]: ejercicio 7.62 (pág. 176).

Actividad 10.21

En una comunidad asamblearia de 100 personas, se presentan 3 para ser elegidas como representantes, con la posibilidad de formar coaliciones. Resulta que 40 prefieren la persona A, 42 la persona B, 45 la persona C, 13 la coalición AB, 20 la coalición BC, 18 la coalición AC y 7 la coalición ABC. Basándonos en esta información, queremos saber:

0. ¿cuántas de dichas 100 personas no votarán a niguna de las personas candidatas, ni individualmente ni en coalición?;
1. ¿cuántas de dichas 100 personas votarán sólo a A?;
2. ¿cuántas de dichas 100 personas votarán sólo a una de las personas candidatas?

Cfr. De la Villa [144]: apéndice 1, problema resuelto 11 (págs. 502–503).

Actividad 10.22

En una comunidad, tras un entrenamiento adecuado, ocurrió que al menos el 70 por ciento mejoró la habilidad A, al menos el 75 por ciento mejoró la habilidad B, como mínimo el 80 por ciento mejoró la habilidad C y al menos el 85 por ciento mejoró la habilidad D. Se nos pregunta, ¿cuántos al menos han mejorado las cuatro habilidades?

[Cubit 79]. *Cfr.* De la Villa [144]: apéndice 1, problema resuelto 12 (pág. 504).

Actividad 10.23

La propiedad esencial de un par ordenado es:

$$\text{si } \langle x_0, x_1 \rangle = \langle y_0, y_1 \rangle, \text{ entonces } x_0 = y_0 \text{ y } x_1 = y_1.$$

0. Se nos propone demostrar que si se define par ordenado, tanto por $\langle x_0, x_1 \rangle = \{\{x\}, \{x, y\}\}$ como por $\langle x_0, x_1 \rangle = \{\{x, 0\}, \{y, 1\}\}$, entonces, en ambos casos, se satisface la propiedad esencial.
1. ¿Cómo se pueden extender estas definiciones para el caso de tuplas triádicas y, en general, para una tupla enádica?

Cfr. Truss [141]: Capítulo 2.1: Sets and relations, Ejercicio 12-15 (pág. 61).

Actividad 10.24

Un centro de análisis de datos y supercómputo (CADS) guarda registro de incidencias de n tipos de error por año. Los datos almacenados son: nombre de la componente, dirección física o lógica de la componente, fecha de fabricación o creación de la componente, fecha(s) de apertura y cierre de la incidencia, tipo de error detectado y tratado y si el tratamiento fue satisfactorio o no. Se nos requiere para:

0. que demos una descripción del producto cartesiano de conjuntos al que pertenecen los registros;
1. que, designando por U_i^n la función proyección, esto es, la que extrae la coordenada iésima de una tupla enádica —$U_i^n(x_0, x_1, x_{n-1}) = x_i$—, expresemos lo siguiente con notación de conjuntos:
    0. el conjunto de componentes que tenían 50 o más meses en el momento de la apertura de la incidencia;
    1. el conjunto de componentes sobre las que se ha abierto incidencia más de una vez;
    2. el conjunto de componentes que tuvieron abierta incidencia por un total de al menos dos semanas;
    3. el conjunto de tipos de error diagnosticados;
    4. el conjunto de tipos de error tratados con éxito.

Cfr. Truss [141]: Capítulo 2.1: *Sets and relations*, Ejercicio 17 (pág. 61).

Actividad 10.25

Sean m y n dos nodos de un árbol enraizado enario. Demostremos que $d_T(m, n) = |m| + |n| - 2|m \wedge n|$ —donde $|x|$ es la profundidad* del nodo x y $m \wedge n$ es el ancestro común más

cercano a m y n (el primer nodo donde se encuentran, al partir de m y n, los caminos enraizados con nodos terminales m y n)— es una métrica[†].

[*] *Vid.* pág. xcvi de esta edición.
[†] *Vid.* definición 10.24 (pág. 565 de esta edición).

§ 10.18 Muestra de ejemplos finales

¡Por el contrario! —continuó Tarará—. Si hubiese sido así, entonces lo sería; y siéndolo, quizá lo fuera; pero como no fue así tampoco lo es asá. ¡Es lógico!

(Lewis CARROLL, *A través del espejo y lo que Alicia encontró al otro lado*, Capítulo 4: Tararí y Tarará. [Traducción de Jaime de Ojeda]).

. . . .

En los dos ejemplos siguientes, hagamos:

0. Formalicemos la argumentación en lógica de juntores, plasmando minuciosamente la estructura interna de cada enunciado que se formaliza, desglosando cada uno de éstos en proposiciones simples y reflejando la interacción entre todas estas últimas. Llamemos A a la forma lógica encontrada.

1. Demostremos, como mínimo vía dos estrategias de la lógica de juntores, que no es una argumentación válida.

2. Para cada una de las dos estrategias que hemos usado en el apartado anterior,

    0. hallemos los contramodelos para A que proporciona,

    1. demostremos que efectivamente son contramodelos para A,

    2. expresemos en español las contraargumentaciones generadas por tales contramodelos que permiten refutar la argumentación.

Aunque a primera vista son de lógica de juntores, los situamos en lógica de clases porque para aclarar las argumentaciones hacia su formalización en lógica de juntores, al aparecer en ellas cuantores, utilizamos la teoría de conjuntos como mediadora en la traducción.

. . . .

Ejemplo 309

«Los algoritmos que nunca deben usarse son los no eficientes socialmente, mientras son libres. Ningún algoritmo libre puede ser eficiente socialmente a menos que haya sido creado por un verdadero esfuerzo comunitario. Sucede además que nadie es capaz de distinguir entre un algoritmo creado por un verdadero esfuerzo comunitario y un algoritmo eficiente socialmente. Por otro lado, no se conoce ningún algoritmo no libre que haya sido creado por un verdadero esfuerzo comunitario y mucho menos que sea eficiente socialmente. Así que, sólo los algoritmos no creados por un verdadero esfuerzo comunitario y los algoritmos no eficientes socialmente y los algoritmos no libres son los que nunca deben usarse».

[EFO 12.6.2020:1a (p.h.e.c.)].

Resolución.— Llamemos $\mathcal{A}$ a esta argumentación.

0. *Formalización de $\mathcal{A}$ en lógica de juntores.*

   - *Variables proposicionales.*

     Considerando como universo de discurso el conjunto de todos los algoritmos, sean estas cuatro variables proposicionales y sus correspondientes proposiciones simples:

     $p \risingdotseq$ «Un algoritmo es eficiente socialmente»,
     $q \risingdotseq$ «Un algoritmo es libre»,
     $r \risingdotseq$ «Un algoritmo puede usarse»,
     $s \risingdotseq$ «Un algoritmo es creado por un verdadero esfuerzo comunitario».

   - *Estructura lógico-gramatical y reescritura de la argumentación.*

     Identificamos cinco oraciones enunciativas y la estructura deductiva de conjunto de premisas $\{\mathcal{O}_0, \mathcal{O}_1, \mathcal{O}_2, \mathcal{O}_3\}$ y conclusión $\mathcal{O}_4$, que identificamos por estar precedida de «así que», un indicador de conclusión, esto es, apunta que la oración que sigue es la conclusión del argumento.

     En la reescritura de la argumentación utilizaremos el conjunto de todos los algoritmos como universal U y los conjuntos definidos por las anteriores proposiciones simples: $P = \{x : x \text{ es un algoritmo eficiente socialmente}\}$, $Q = \{x : x \text{ es un algoritmo libre}\}$, $R = \{x : x \text{ es un algoritmo que puede usarse}\}$ y $S = \{x : x \text{ es un algoritmo creado por un verdadero esfuerzo comunitario}\}$.

     Tenemos así:

$\mathcal{O}_0$, es decir, «los algoritmos que nunca deben usarse son los no eficientes socialmente, mientras son libres» —esto es, «ningún x que no sea de P y que sea de Q es de R» ≡ «cualquier x que no sea de P y sea de Q no es de R» ≡ $P^{\complement} \cap Q \subseteq R^{\complement}$—, la reescribimos como «si un algoritmo es no eficiente socialmente y libre, entonces, nunca debe usarse», interpretación cuya fórmula correspondiente inmediata en la lógica de juntores es $\neg p \wedge q \rightarrow \neg r$ —o cualquier fórmula equivalente, por ejemplo, $q \rightarrow (\neg p \rightarrow \neg r)$, que se interpreta así: «si un algoritmo es libre, entonces, no debe usarse si no es eficiente socialmente»—;

$\mathcal{O}_1$, es decir, «ningún algoritmo libre puede ser eficiente socialmente a menos que haya sido creado por un verdadero esfuerzo comunitario» —esto es, «ningún x de Q es de P a menos que sea de S» ≡ «cualquier x de Q que no sea de S, no es de P» ≡ «si x es de Q y no es de S, entonces, no es de P» ≡ $Q \cap S^{\complement} \subseteq P^{\complement}$—, la reescribimos como «si un algoritmo es libre y no ha sido creado por un verdadero esfuerzo comunitario, entonces, no es eficiente socialmente», interpretación cuya fórmula correspondiente inmediata en la lógica de juntores es $q \wedge \neg s \rightarrow \neg p$;

$\mathcal{O}_2$, es decir, «nadie es capaz de distinguir entre un algoritmo creado por un verdadero esfuerzo comunitario y un algoritmo eficiente socialmente», la reescribimos como «en la práctica, que un algoritmo haya sido creado por un verdadero esfuerzo comunitario y que un algoritmo sea eficiente socialmente, son equivalentes», interpretación cuya fórmula correspondiente inmediata en la lógica de juntores es $s \leftrightarrow p$;

$\mathcal{O}_3$, es decir, «no se conoce ningún algoritmo no libre que haya sido creado por un verdadero esfuerzo comunitario y mucho menos que sea eficiente socialmente» —esto es, «si x es de S o es de P, entonces, x es de Q» ≡ $S \cup P \subseteq Q$ ≡ $Q^{\complement} \subseteq (S \cup P)^{\complement}$ ≡ $Q^{\complement} \subseteq (S^{\complement} \cap P^{\complement})$), de cualquiera de estas formas—, de reescritura inmediata como «no se conoce ningún algoritmo no libre que haya sido creado por un verdadero esfuerzo comunitario y tampoco se conoce ningún algoritmo no libre que sea eficiente socialmente», que tiene por correspondiente la fórmula de la lógica de juntores —esto es, $((Q^{\complement} \cap S)^{\complement} \cap (Q \cap P)^{\complement})$—, que reescribimos como «si un algoritmo es no libre, entonces, ni ha sido creado por un verdadero esfuerzo comunitario ni es eficiente socialmente», interpretación cuya fórmula correspondiente inmediata en la lógica de juntores es $\neg q \rightarrow \neg(s \vee p)$;

$\mathcal{O}_4$, es decir, «sólo los algoritmos no creados por un verdadero esfuerzo comunitario y los algoritmos no eficientes socialmente y los algoritmos no libres son los que nunca deben usarse» —esto es, «sólo los x de $S^{\complement}$ y los de $P^{\complement}$ y los de $Q^{\complement}$ son los de $R^{\complement}$» ≡ «ningún x que no sea de $S^{\complement}$ o de $P^{\complement}$ o de $Q^{\complement}$ es de $R^{\complement}$» ≡ «todos los de $R^{\complement}$ son de $S^{\complement}$ o de $P^{\complement}$ o de $Q^{\complement}$» ≡ «si es de $R^{\complement}$, entonces, es de $S^{\complement}$ o de $P^{\complement}$ o de $Q^{\complement}$»—, la reescribimos como «si un algoritmo es de los que nunca deben usarse, entonces, no ha sido

creado por un verdadero esfuerzo comunitario o no es eficiente socialmente o no es libre», interpretación cuya fórmula correspondiente inmediata en la lógica de juntores es $\neg r \to \neg s \vee \neg p \vee \neg q$.

- *Forma lógica*.

  Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1, \phi_2, \phi_3\} = \{\neg p \wedge q \to \neg r, q \wedge \neg s \to \neg p, s \leftrightarrow p, \neg q \to \neg(s \vee p)\}$, con cuatro premisas, y la conclusión ψ, a saber, $\neg r \to \neg s \vee \neg p \vee \neg q$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $(\neg p \wedge q \to \neg r) \wedge (q \wedge \neg s \to \neg p) \wedge (s \leftrightarrow p) \wedge (\neg q \to \neg(s \vee p)) \to (\neg r \to \neg s \vee \neg p \vee \neg q)$; llamémosla A.

1. *Demostración de la no validez de $\mathcal{A}$ mediante, como mínimo, dos estrategias de la lógica de juntores*.

Elegimos formas normales como primera estrategia y tablas semánticas como segunda.

A. **Estrategia 0. Formas normales.**

I. La fórmula A, reescrita como $\neg p \vee \neg q \vee r \vee \neg s$, está en forma normal conjuntiva (FNC) (mínima); observamos que sólo tiene una cláusula y como en ella no aparece una variable y su negación, A no es una fórmula válida, es decir, es una contingencia o una fórmula insatisfactible.

II. La fórmula A, reescrita como $\neg p \vee \neg q \vee r \vee \neg s$, está en forma normal disyuntiva (FND) (mínima); observamos que tiene cuatro cubos y en ninguno de ellos aparece una variable y su negación, por lo que no es una fórmula insatisfactible, es decir, es una fórmula válida o una contingencia.

De I y II, se sigue que la fórmula A es una contingencia.

Por lo tanto, $\mathcal{A}$ no es una argumentación válida.

B. **Estrategia 1. Tablas semánticas.**

I. *Identificación del conjunto Γ*.

De acuerdo con la libertad que expone la nota de la entradilla (pág. 283), identificamos la estructura de $\mathcal{A}$ con la deducción semántica $\{\phi_0, \phi_1, \phi_2, \phi_3\} \vDash \psi$. Refutar $\{\phi_0, \phi_1, \phi_2, \phi_3\} \vDash \psi$ es demostrar que $\phi_0 \wedge \phi_1 \wedge \phi_2 \wedge \phi_3 \wedge \neg\psi$ es una fórmula válida.

Correspondiendo a dicha estructura deductiva, definimos $\Gamma = \{\phi_0, \phi_1, \phi_2, \phi_3\} \cup \{\neg\psi\} = \{\neg p \wedge q \to \neg r, q \wedge \neg s \to \neg p, s \leftrightarrow p, \neg q \to \neg(s \vee p), \neg(\neg r \to (\neg s \vee \neg p) \vee \neg q)\}$. Estudiemos si existe una refutación para Γ, esto es, si la tabla semántica (el árbol para Γ) es un árbol insatisfactible, un árbol de refutación, para Γ.

II. *Construcción anotada del árbol semántico*.

Veamos el árbol generado por Tree Proof Generator en la figura 10.1 (pág. 577 de esta edición).

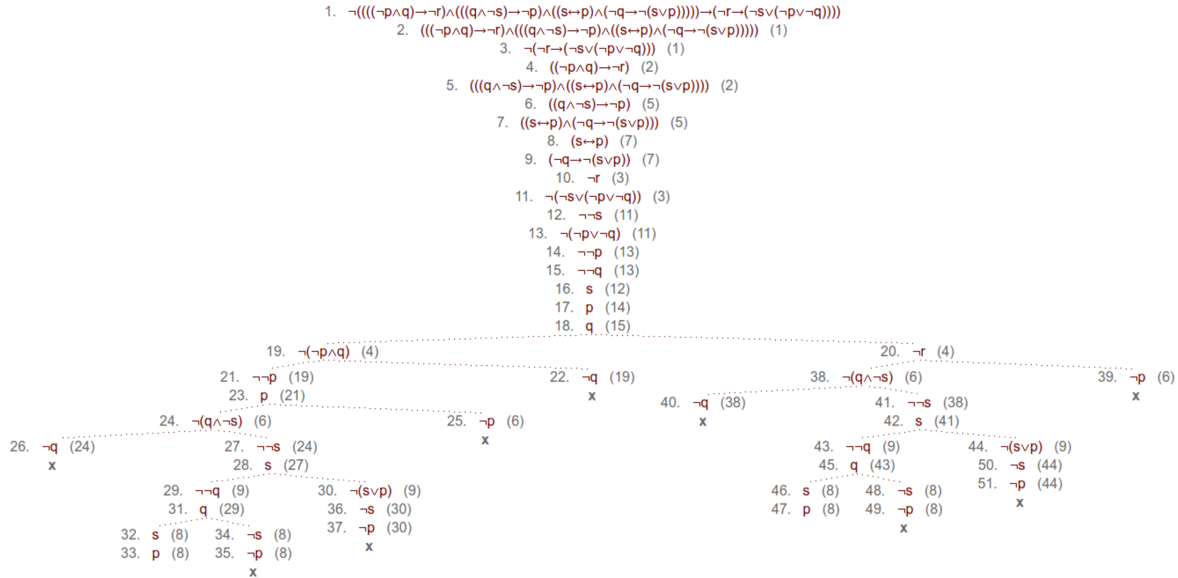


Figura 10.1.— Árbol semántico correspondiente a Γ que genera el artefacto en línea Tree Proof Generator (versión *oldtrees*) con la entrada `((((\lnot p \wedge q) \to \lnot r) \wedge ((q \wedge \lnot s) \to \lnot p) \wedge (s \leftrightarrow p) \wedge (\lnot q \to \lnot (s \vee p))) \to (\lnot r \to (\lnot s \vee \lnot p \vee \lnot q)))`.

III. *Demostración de que es un árbol terminado*.

El tronco de este árbol es $\rho_0 = \{\neg((((\neg p \wedge q) \to \neg r) \wedge ((q \wedge \neg s) \to \neg p) \wedge (s \leftrightarrow p) \wedge (\neg q \to \neg(s \vee p))) \to (\neg r \to (\neg s \vee \neg p \vee \neg q))), ((\neg p \wedge q) \to \neg r) \wedge ((q \wedge \neg s) \to \neg p) \wedge (s \leftrightarrow p) \wedge (\neg q \to \neg(s \vee p)), \neg(\neg r \to (\neg s \vee \neg p \vee \neg q)), (\neg p \wedge q) \to \neg r, ((q \wedge \neg s) \to \neg p) \wedge (s \leftrightarrow p) \wedge (\neg q \to \neg(s \vee p)), (q \wedge \neg s) \to \neg p, (s \leftrightarrow p) \wedge (\neg q \to \neg(s \vee p)), s \leftrightarrow p, \neg q \to \neg(s \vee p), \neg r, \neg(\neg s \vee (\neg p \vee \neg q)), \neg\neg s, \neg(\neg p \vee \neg q), \neg\neg p, \neg\neg q, s, p, q\}$, y sus once ramas son:

$\rho_1 = \rho_0 \cup \{\neg(\neg p \wedge q), \neg\neg p, p, \neg(q \wedge \neg s), \neg q\}$,

$\rho_2 = \rho_0 \cup \{\neg(\neg p \wedge q), \neg\neg p, p, \neg(q \wedge \neg s), \neg\neg s, s, \neg\neg q, q, s, p\}$,

$\rho_3 = \rho_0 \cup \{\neg(\neg p \wedge q), \neg\neg p, p, \neg(q \wedge \neg s), \neg\neg s, s, \neg\neg q, q, \neg s, \neg p\}$,

$\rho_4 = \rho_0 \cup \{\neg(\neg p \wedge q), \neg\neg p, p, \neg(q \wedge \neg s), \neg\neg s, s, \neg(s \vee p), \neg s, \neg p\}$,

$\rho_5 = \rho_0 \cup \{\neg(\neg p \wedge q), \neg\neg p, p, \neg p\}$,

$\rho_6 = \rho_0 \cup \{\neg(\neg p \wedge q), \neg q\}$,

$\rho_7 = \rho_0 \cup \{\neg r, \neg(q \wedge \neg s), \neg q\}$,

$\rho_8 = \rho_0 \cup \{\neg r, \neg(q \wedge \neg s), \neg\neg s, s, \neg\neg q, q, s, p\}$,

$\rho_9 = \rho_0 \cup \{\neg r, \neg(q \wedge \neg s), \neg\neg s, s, \neg\neg q, q, \neg s, \neg p\}$,

$\rho_{10} = \rho_0 \cup \{\neg r, \neg(q \wedge \neg s), \neg\neg s, s, \neg(s \vee p), \neg s, \neg p\}$,
$\rho_{11} = \rho_0 \cup \{\neg r, \neg p\}$.

Es un árbol terminado, pues toda rama es insatisfactible o completa; en efecto, por un lado, $\rho_1, \rho_3, \rho_4, \rho_5, \rho_6, \rho_7, \rho_9, \rho_{10}$ y ρ_{11} son ramas insatisfactibles, al existir en cada una de ellas al menos una variable y su negación, p y $\neg p$ en $\rho_3, \rho_4, \rho_5, \rho_9, \rho_{10}$ y ρ_{11}, y q y $\neg q$ en ρ_1, ρ_6, ρ_7, y por otro, las ramas ρ_2 y ρ_8, aunque son satisfactibles (ya que son conjuntos satisfactibles de fórmulas [no contienen una variable y su negación]), son completas.

Veamos que ρ_2 es una rama completa —un análisis similar para ρ_8, demostraría que también lo es—. Para ello, comprobemos que si una fórmula conjuntiva (de tipo α) pertenece a ρ_2, entonces también pertenecen a ρ_2 sus dos conjuntos y que si una fórmula disyuntiva (de tipo β) pertenece a ρ_2, entonces también pertenece a ρ_2 alguno de sus disyuntos:

0. con respecto a la fórmula conjuntiva $\neg((((\neg p \wedge q) \rightarrow \neg r) \wedge ((q \wedge \neg s) \rightarrow \neg p) \wedge (s \leftrightarrow p) \wedge (\neg q \rightarrow \neg(s \vee p))) \rightarrow (\neg r \rightarrow (\neg s \vee \neg p \vee \neg q)))$ (nodo 1), tanto $((\neg p \wedge q) \rightarrow \neg r) \wedge ((q \wedge \neg s) \rightarrow \neg p) \wedge (s \leftrightarrow p) \wedge (\neg q \rightarrow \neg(s \vee p))$ como $(\neg r \rightarrow (\neg s \vee \neg p \vee \neg q))$ pertenecen al tronco ρ_0 (nodos 2 y 3, respectivamente) y por tanto, pertenecen a ρ_2;

1. con respecto a la fórmula conjuntiva $((\neg p \wedge q) \rightarrow \neg r) \wedge ((q \wedge \neg s) \rightarrow \neg p) \wedge (s \leftrightarrow p) \wedge (\neg q \rightarrow \neg(s \vee p))$ (nodo 2), tanto $(\neg p \wedge q) \rightarrow \neg r$ como $(q \wedge \neg s) \rightarrow \neg p$ como $s \leftrightarrow p$ como $\neg q \rightarrow \neg(s \vee p)$, pertenecen al tronco ρ_0 (nodos 4, 6, 8 y 9, respectivamente) y por tanto, pertenecen a ρ_2;

2. con respecto a la fórmula conjuntiva $\neg(\neg r \rightarrow (\neg s \vee \neg p \vee \neg q)))$ (nodo 3), $\neg r \in \rho_0 \subset \rho_2$ (nodo 10) y $\neg(\neg s \vee (\neg p \vee \neg q)) \in \rho_0 \subset \rho_2$ (nodo 11);

3. con respecto a la fórmula disyuntiva $(\neg p \wedge q) \rightarrow \neg r$ (nodo 4), $\neg r \in \rho_0 \subset \rho_2$ (nodo 10)

4. con respecto a la fórmula conjuntiva $((q \wedge \neg s) \rightarrow \neg p) \wedge (s \leftrightarrow p) \wedge (\neg q \rightarrow \neg(s \vee p))$ (nodo 5), $((q \wedge \neg s) \rightarrow \neg p) \in \rho_0 \subset \rho_2$ (nodo 6), $(s \leftrightarrow p) \in \rho_0 \subset \rho_2$ (nodo 8) y y $(\neg q \rightarrow \neg(s \vee p)) \in \rho_0 \subset \rho_2$ (nodo 9);

5. con respecto a la fórmula disyuntiva $(q \wedge \neg s) \rightarrow \neg p$ (nodo 6), $\neg(q \wedge \neg s) \in \rho_2$ (nodo 24);

6. con respecto a la fórmula conjuntiva $(s \leftrightarrow p) \wedge (\neg q \rightarrow \neg(s \vee p))$ (nodo 7), $(s \leftrightarrow p) \in \rho_0 \subset \rho_2$ (nodo 8) y $(\neg q \rightarrow \neg(s \vee p)) \in \rho_0 \subset \rho_2$ (nodo 9);

7. con respecto a la fórmula disyuntiva $s \leftrightarrow p$ (nodo 8), $s \wedge p \in \rho_2$ (nodo 31,5, entre el 31 y el 32, no aparece en la fig. [$s \leftrightarrow p \equiv (s \wedge p) \vee (\neg s \wedge \neg p)$]);

8. con respecto a la fórmula disyuntiva $\neg q \rightarrow \neg(s \vee p)$ (nodo 9), $\neg\neg q \in \rho_0 \subset \rho_2$ (nodo 15);

9. con respecto a la fórmula conjuntiva $\neg(\neg s \vee (\neg p \vee \neg q)))$ (nodo 11), $\neg\neg s \in \rho_0 \subset \rho_2$ (nodo 12) y $\neg(\neg p \vee \neg q)$ (nodo 13);

10. con respecto a la fórmula conjuntiva $\neg\neg s$ (nodo 12), $s \in \rho_0 \subset \rho_2$ (nodo 16);

11. con respecto a la fórmula conjuntiva $\neg(\neg p \vee \neg q)$ (nodo 13), $\neg\neg p \in \rho_0 \subset \rho_2$ (nodo 14) y $\neg\neg q \in \rho_0 \subset \rho_2$ (nodo 15);

12. con respecto a la fórmula conjuntiva $\neg\neg p$ (nodo 14), $p \in \rho_0 \subset \rho_2$ (nodo 17);

13. con respecto a la fórmula disyuntiva $\neg(\neg p \wedge q)$ (nodo 19), $\neg\neg p \in \rho_2$ (nodo 21);

14. con respecto a la fórmula conjuntiva $\neg\neg p$ (nodo 21), $p \in \rho_2$ (nodo 23);

15. con respecto a la fórmula disyuntiva $\neg(q \wedge \neg s)$ (nodo 24), $\neg\neg s \in \rho_2$ (nodo 27);

16. finalmente, con respecto a la fórmula conjuntiva $\neg\neg s$ (nodo 27), $s \in \rho_2$ (nodo 28).

IV. *Demostración de la validez o no de $\mathcal{A}$.*

Como ρ_2 es una rama satisfactible, este árbol terminado es satisfactible, por lo tanto, no existe una refutación para Γ, por lo que, por el teorema 3.8 (pág. 281 de esta edición), de Φ, no se deduce ψ, de donde, la argumentación $\mathcal{A}$ no es válida.

2. Veamos.

A. **Estrategia 0. Formas normales.**

0. *Identificación de los contramodelos para A generados.*

La expresión de A en FNC, $\neg p \vee \neg q \vee r \vee \neg s$, proporciona un contramodelo para A, a saber, $I(p) = 1$, $I(q) = 1$, $I(r) = 0$, $I(s) = 1$, o abreviadamente, I_{1101} —su expresión en FND, $\neg p \vee \neg q \vee r \vee \neg s$, por otra parte, proporciona múltiples modelos para la satisfactibilidad de A, a saber, todas aquellas interpretaciones en las que $I(p) = 0$ o $I(q) = 0$ o $I(r) = 1$ o $I(s) = 0$—.

1. *Demostración de que los contramodelos lo son para A.*

No es difícil demostrar que I_{1101} es un contramodelo para A; para ello, estudiemos la valoración de verdad de A con dicha interpretación:

$pqrs$	$(((((\neg p \wedge q) \rightarrow \neg r) \wedge ((q \wedge \neg s) \rightarrow \neg p)) \wedge (s \leftrightarrow p)) \wedge (\neg q \rightarrow (\neg s \vee p))) \rightarrow (\neg r \rightarrow ((\neg s \vee \neg p) \vee \neg q))$
1101	0 1 0 1 1 1 0 1 1 0 0 1 1 0 1 1 1 1 1 1 0 1 1 0 1 1 1 $\boxed{0}$ 1 0 0 0 1 0 0 1 0 0 1

2. *Expresión en español de las contraargumentaciones proporcionadas por los contramodelos.*

El contramodelo hallado permite refutar $\mathcal{A}$, ya que el hecho de disponer de un algoritmo eficiente socialmente, libre y creado por un verdadero esfuerzo comunitario, a la vez que no deba usarse, es suficiente para que se satisfagan las premisas y no se satisfaga la conclusión, ya que es precisamente un contraejemplo a lo que se afirma en ella.

La argumentación $\mathcal{A}$ es una interpretación de la forma lógica A que hemos determinado para $\mathcal{A}$. Una contrargumentación de $\mathcal{A}$ es una argumentación en la misma forma lógica que $\mathcal{A}$, esto es, una re-interpretación de A, tal que sus premisas son verdaderas y su conclusión es falsa.

Una contraargumentación es Pr0 ∧ Pr1 ∧ Pr2 ∧ Pr3 ∧ ¬ Co, donde algoritmo-1101 denota un algoritmo eficiente socialmente, libre, creado por un verdadero esfuerzo comunitario y que no debe usarse (la + en el dibujo de abajo):

Pr0: Los algoritmos-1101 que nunca deben usarse son los no eficientes socialmente, mientras son libres. (V)

Pr1: [$\mathcal{O}_1$] Ningún algoritmo-1101 libre puede ser eficiente socialmente a menos que haya sido creado por un verdadero esfuerzo comunitario. (V)

Sucede además que

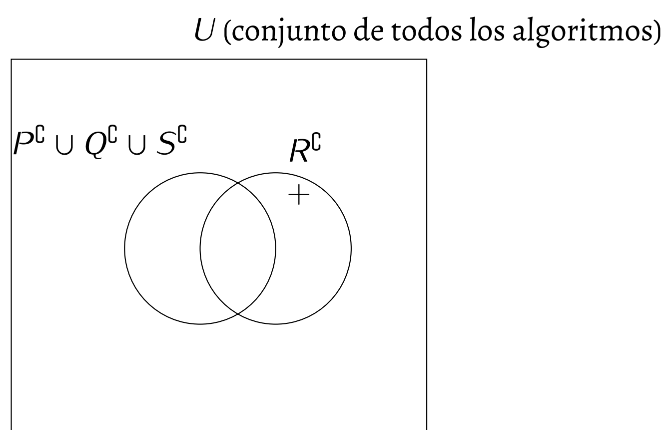
Pr2: nadie es capaz de distinguir entre un algoritmo-1101 creado por un verdadero esfuerzo comunitario y un algoritmo-1101 eficiente socialmente. (V)

Por otro lado,

Pr3: no se conoce ningún algoritmo-1101 no libre que haya sido creado por un verdadero esfuerzo comunitario y mucho menos que sea eficiente socialmente. (V)

Así que,

Co: sólo los algoritmos-1101 no creados por un verdadero esfuerzo comunitario y los algoritmos-1101 no eficientes socialmente y los algoritmos-1101 no libres son los que nunca deben usarse. (F)



B. **Estrategia 1. Tablas semánticas.**

0. *Identificación de los modelos para* Γ *que proporcionan las ramas satisfactibles.*

   Al ser ρ_2 y ρ_8 ramas satisfactibles, proporcionan modelos para el conjunto Γ —esto es, contramodelos para A—. De hecho, ρ_2 y ρ_8 proporcionan el mismo modelo —y como no podía ser de otra forma, el mismo contramodelo para A que proporcionó la expresión de A en FNC—, a saber, I_{1101} (veamos, por ejemplo, los nodos troncales 17, 18, 10 y 16).

1. *Demostración de que los modelos lo son para* Γ.

   No es difícil demostrar que I_{1101} es un modelo para Γ; para ello, estudiemos las valoraciones de verdad de las fórmulas de Γ con dicha interpretación:

p q r s	$(\neg\, p \wedge q) \rightarrow \neg\, r$	$(q \wedge \neg\, s) \rightarrow \neg\, p$	$s \leftrightarrow p$
1 1 0 1	0 1 0 1 $\boxed{1}$ 1 0	1 0 0 1 $\boxed{1}$ 0 1	1 $\boxed{1}$ 1

p q r s	$\neg\, q \rightarrow \neg\,(s \vee p)$	$\neg\,(\neg\, r \rightarrow ((\neg\, s \vee \neg\, p) \vee \neg\, q))$
1 1 0 1	0 1 $\boxed{1}$ 0 1 1 1	$\boxed{1}$ 1 0 0 0 1 0 0 1 0 0 1

2. *Expresión en español de las contraargumentaciones proporcionadas por los modelos.*

   Recordemos: un modelo para Γ es un contramodelo para A. Después de haber recordado esto, *vid. supra* el apartado 2.A.2 de este mismo esquema de resolución. ■

Observación 10.18.0.— Dado que éste ha sido el último ejemplo de formalización lógica de «a menos que» en estas notas, diremos que hasta este momento nos hemos guiado por los aspectos exclusivos de la lógica clásica, a saber, sintáctico (la relación de los signos entre sí) y semántico (la relación entre los signos y lo significado por ellos); si hubiésemos incluido el aspecto pragmático (la relación entre los signos y la conducta) seguramente hubiésemos empleado la contravalencia en vez de la disyunción (pues aquella está fuertemente implícita en nuestra práctica social de «a menos que») y hubiésemos intrepretado «sucede p a menos que suceda q» como «si no sucede q, entonces sucede p y si sucede q, entonces no sucede p», esto es, como $p \veebar q$ en vez de $p \vee q$. Otro

ejemplo: «si sucede p entonces sucede q a menos que suceda r», que hubiésemos formalizado $\neg p \vee q \vee r$ exclusivamente desde los aspectos sintácticos y semánticos, pero desde la pragmática seguramente hubiésemos considerado su equivalencia a «si sucede p y no sucede r entonces sucede q, y si sucede p y sucede r entonces no sucede q», esto es, lo hubiésemos formalizado como $(p \wedge \neg r \to q) \wedge (p \wedge r \to \neg q)$, fórmula lógicamente equivalente a $\neg p \vee (q \veebar r)$. Lo dicho sirve tanto para «a menos que» como para otras expresiones equivalentes en nuestra lengua, por ejemplo, para «excepto si».

Ejemplo 310

> «Todos hacen lo que tú dices o lo que yo digo, aunque algunos de los tramposos no hacen lo que tú dices. Sin embargo, los que hacen lo que tú dices y los robots hacen lo que yo digo, y además, nadie de los tramposos deja nunca de hacer lo que yo digo. En fin, que no todos los que hacen lo que tú dices, hacen lo que yo digo».
>
> [EFE 14.7.2020:1a (p.h.e.c.)].

Resolución.— Llamemos $\mathcal{A}$ a esta argumentación.

0. *Formalización de $\mathcal{A}$ en lógica de juntores.*

- *Variables proposicionales.*

  Considerando como universo de discurso el conjunto de todos los seres (humanos, robots...) y la poca expresividad de la lógica de juntores, sean estas cuatro variables proposicionales y sus correspondientes proposiciones simples:

$$p \leftrightharpoons \text{«Un ser hace lo que tú dices»},$$
$$q \leftrightharpoons \text{«Un ser hace lo que yo digo»},$$
$$r \leftrightharpoons \text{«Un ser hace trampas»},$$
$$s \leftrightharpoons \text{«Un ser es un robot»}.$$

- *Estructura lógico-gramatical y reescritura de la argumentación.*

  Identificamos tres oraciones enunciativas y la estructura deductiva de conjunto de premisas $\{\mathcal{O}_0, \mathcal{O}_1\}$ y conclusión $\mathcal{O}_2$, que identificamos por estar precedida de «en fin», un indicador de conclusión, esto es, apunta que la oración que sigue es la conclusión del argumento.

  En la reescritura de la argumentación utilizaremos el conjunto de todos los seres como universal U y los conjuntos definidos por las anteriores proposiciones simples: $P = \{x : x \text{ hace lo que tú dices}\}$, $Q = \{x : x \text{ hace lo que yo digo}\}$, $R = \{x : x \text{ hace trampas}\}$ y $S = \{x : x \text{ es un robot}\}$.

Tenemos así:

$\mathcal{O}_0$, es decir, «todos hacen lo que tú dices o lo que yo digo, aunque algunos de los tramposos no hacen lo que tú dices», en la que a su vez identificamos «todos hacen lo que tú dices o lo que yo digo» ($\mathcal{O}_{0a}$) y «algunos de los tramposos no hacen lo que tú dices» ($\mathcal{O}_{0b}$) unidas por la conjunción adversativa «aunque» ($\mathcal{O}_{0a} \wedge \mathcal{O}_{0b}$):

$\mathcal{O}_{1a}$, esto es, «todo x que sea de U es de P o de Q» $\equiv P \cup Q \subseteq U \equiv P \cup Q = U$, interpretación conjuntista cuya fórmula correspondiente inmediata en la lógica de juntores es $p \vee q \leftrightarrow \top$ —o cualquier fórmula equivalente, por ejemplo, $\neg(p \vee q) \leftrightarrow \neg\top$ o $(\neg p \wedge \neg q) \leftrightarrow \bot$ o simplemente $p \vee q$—;

$\mathcal{O}_{1b}$, esto es, «hay algún x de R que no es de P» $\equiv R \cap \complement P \neq \emptyset$, interpretación conjuntista cuya fórmula correspondiente inmediata en la lógica de juntores es $\neg((r \wedge \neg p) \leftrightarrow \bot)$ —o cualquier fórmula equivalente, por ejemplo, $\neg(r \to p)$ o simplemente $r \wedge \neg p$—.

En definitiva, $\mathcal{O}_0$ se formaliza en lógica de juntores como $((p \vee q) \leftrightarrow \top) \wedge \neg((r \wedge \neg p) \leftrightarrow \bot)$ —o cualquier fórmula equivalente, por ejemplo, $\neg p \wedge q \wedge r$.

$\mathcal{O}_1$, es decir, «los que hacen lo que tú dices y los robots hacen lo que yo digo, y además, nadie de los tramposos deja nunca de hacer lo que yo digo», en la que a su vez, identificamos «los que hacen lo que tú dices y los robots hacen lo que yo digo» ($\mathcal{O}_{1a}$) y «nadie de los tramposos deja nunca de hacer lo que yo digo» ($\mathcal{O}_{1b}$) unidas por la conjunción copulativa «y» ($\mathcal{O}_{1a} \wedge \mathcal{O}_{1b}$):

$\mathcal{O}_{1a}$, esto es, «todo x que sea de P o de S, es de Q» $\equiv P \cup S \subseteq Q$, interpretación conjuntista cuya fórmula correspondiente inmediata en la lógica de juntores es $p \vee s \to q$ —o cualquier fórmula equivalente, por ejemplo, $\neg(p \vee s) \vee q$.

$\mathcal{O}_{1b}$, esto es, «no hay ningún x que sea de R y no sea de Q» $\equiv$ «si x pertenece a R, entonces pertenece a Q» $\equiv R \subseteq Q$, interpretación conjuntista cuya fórmula correspondiente inmediata en la lógica de juntores es $r \to q$ —o cualquier fórmula equivalente, por ejemplo, $\neg r \vee q$.

En definitiva, $\mathcal{O}_1$ se formaliza en lógica de juntores por $(p \vee s \to q) \wedge (r \to q)$ —o por cualquier fórmula equivalente, por ejemplo, $\neg(p \vee r \vee s) \vee q$.

$\mathcal{O}_2$, es decir, «no todos los que hacen lo que tú dices, hacen lo que yo digo», esto es, «es falso que todo x de P sea de Q» $\equiv P \nsubseteq Q$, interpretación conjuntista cuya fórmula correspondiente inmediata en la lógica de juntores es $\neg(p \to q)$ —o cualquier fórmula equivalente, por ejemplo, $p \wedge \neg q$.

- *Forma lógica*.

Identificamos el conjunto de premisas $\Phi = \{\phi_0, \phi_1\} = \{((p \vee q) \leftrightarrow 1) \wedge \neg((r \wedge \neg p) \leftrightarrow 0), ((p \vee s) \rightarrow q) \wedge (r \rightarrow q)\}$, con cuatro premisas, y la conclusión ψ, a saber, $\neg(p \rightarrow q)$. La fórmula correspondiente a $\mathcal{A}$ en lógica de juntores es $((((p \vee q) \leftrightarrow 1) \wedge \neg((r \wedge \neg p) \leftrightarrow 0)) \wedge (((p \vee s) \rightarrow q) \wedge (r \rightarrow q))) \rightarrow \neg(p \rightarrow q)$ (llamémosla A) (o cualquier fórmula equivalente, por ejemplo, $\neg p \wedge q \wedge r \wedge (\neg p \vee q) \wedge (q \vee \neg r) \wedge (q \vee \neg s) \rightarrow p \wedge \neg q$).

1. *Demostración de la no validez de $\mathcal{A}$ mediante, como mínimo, dos estrategias de la lógica de juntores*.

Elegimos formas normales como primera estrategia y tablas de verdad (como estrategia de verificación) como segunda.

A. **Estrategia 0. Formas normales.**

I. La fórmula A, reescrita como $(p \vee \neg q \vee \neg r \vee s) \wedge (p \vee \neg q \vee \neg r \vee \neg s)$, está en forma normal conjuntiva (FNC); observamos que tiene dos cláusulas y como en ellas no aparece una variable y su negación, A no es una fórmula válida, es decir, es una contingencia o una fórmula insatisfactible.

II. La fórmula A, reescrita como $p \vee \neg q \vee \neg r$, está en forma normal disyuntiva (FND) (mínima); observamos que tiene tres cubos y en ninguno de ellos aparece una variable y su negación, por lo que no es una fórmula insatisfactible, es decir, es una fórmula válida o una contingencia.

De I y II, se sigue que la fórmula A es una contingencia.

Por lo tanto, $\mathcal{A}$ no es una argumentación válida.

B. **Estrategia 1. Tablas de verdad.**

De la tabla de verdad de A,

p q r s	(((((p ∨ q) ↔ ⊤) ∧ ¬ ((r ∧ ¬ p) ↔ ⊥))∧((p ∨ s) → q))∧(r → q))→ ¬ (p → q)
1 1 1 1	1 1 1 1 1 0 0 1 0 0 1 1 0 0 1 1 1 1 1 0 1 1 1 1 0 1 1 1
1 1 1 0	1 1 1 1 1 0 0 1 0 0 1 1 0 0 1 1 0 1 1 0 1 1 1 1 0 1 1 1
1 1 0 1	1 1 1 1 1 0 0 0 0 0 1 1 0 0 1 1 1 1 1 0 0 1 1 1 0 1 1 1
1 1 0 0	1 1 1 1 1 0 0 0 0 0 1 1 0 0 1 1 0 1 1 0 0 1 1 1 0 1 1 1
1 0 1 1	1 1 0 1 1 0 0 1 0 0 1 1 0 0 1 1 1 0 0 0 1 0 0 1 1 1 0 0
1 0 1 0	1 1 0 1 1 0 0 1 0 0 1 1 0 0 1 1 0 0 0 0 1 0 0 1 1 1 0 0
1 0 0 1	1 1 0 1 1 0 0 0 0 0 1 1 0 0 1 1 1 0 0 0 0 1 0 1 1 1 0 0
1 0 0 0	1 1 0 1 1 0 0 0 0 0 1 1 0 0 1 1 0 0 0 0 0 1 0 1 1 1 0 0
0 1 1 1	0 1 1 1 1 1 1 1 1 1 0 0 0 1 0 1 1 1 1 1 1 1 1 $\boxed{0}$ 0 0 1 1
0 1 1 0	0 1 1 1 1 1 1 1 1 1 0 0 0 1 0 0 0 1 1 1 1 1 1 $\boxed{0}$ 0 0 1 1
0 1 0 1	0 1 1 1 1 0 0 0 0 1 0 1 0 0 0 1 1 1 1 0 0 1 1 1 0 0 1 1
0 1 0 0	0 1 1 1 1 0 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0 1 1 1 0 0 1 1
0 0 1 1	0 0 0 0 1 0 1 1 1 1 0 0 0 0 0 1 1 0 0 0 1 0 0 1 0 0 1 0
0 0 1 0	0 0 0 0 1 0 1 1 1 1 0 0 0 0 0 0 0 1 0 0 1 0 0 1 0 0 1 0
0 0 0 1	0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 1 1 0 0 0 0 1 0 1 0 0 1 0
0 0 0 0	0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 1 0 0 0 1 0 1 0 0 1 0

se sigue que A es una contingencia (para las interpretaciones I_{0111} e I_{0110}, A es falsa). Por lo tanto, la argumentación $\mathcal{A}$ no es válida.

2. Veamos.

   A. **Estrategia 0. Formas normales.**

      0. *Identificación de los contramodelos para A generados.*

         La expresión en FNC de A, $(p \vee \neg q \vee \neg r \vee s) \wedge (p \vee \neg q \vee \neg r \vee \neg s)$, proporciona dos contramodelos para A, a saber, $I(p) = 0$, $I(q) = 1$, $I(r) = 1$, $I(s) = 1$ e $I(p) = 0$, $I(q) = 1$, $I(r) = 1$, $I(s) = 0$, o abreviadamente, I_{0111} e I_{0110} —la expresión en FND de A, $p \vee \neg q \vee \neg r$, por otra parte, proporciona múltiples modelos para la satisfactibilidad de A, a saber, todas aquellas interpretaciones en las que $I(p) = 1$ o $I(q) = 0$ o $I(r) = 0$—.

      1. *Demostración de que los contramodelos lo son para A.*

         Ya lo demostramos al hacer la tabla de verdad. En cualquier caso, destaquemos de nuevo las valoraciones de verdad de A con las interpretaciones I_{0110} y I_{0111}:

p q r s	(((((p ∨ q) ↔ ⊤) ∧ ¬ ((r ∧ ¬ p) ↔ ⊥))∧((p ∨ s) → q))∧(r → q))→ ¬ (p → q)
0 1 1 1	0 1 1 1 1 1 1 1 1 1 0 0 0 1 0 1 1 1 1 1 1 1 1 $\boxed{0}$ 0 0 1 1
0 1 1 0	0 1 1 1 1 1 1 1 1 1 0 0 0 1 0 0 0 1 1 1 1 1 1 $\boxed{0}$ 0 0 1 1

      2. *Expresión en español de las contraargumentaciones proporcionadas por los contramodelos.*

La argumentación $\mathcal{A}$ es una interpretación de la forma lógica A que hemos determinado para $\mathcal{A}$. Una contrargumentación de $\mathcal{A}$ es una argumentación en la misma forma lógica que $\mathcal{A}$, esto es, una re-interpretación de A, tal que sus premisas son verdaderas y su conclusión es falsa.

Los contramodelos hallados permiten refutar $\mathcal{A}$. En efecto:

- Por un lado, el contramodelo I_{0111} así lo permite, ya que el hecho de que exista un robot tramposo que haga lo que yo digo pero que no haga lo que tú dices, es suficiente para que se satisfagan las premisas y no se satisfaga la conclusión, ya que es precisamente un contraejemplo a lo que se afirma en ella; de hecho, una contraargumentación es $Pr_{0a} \wedge Pr_{0b} \wedge Pr_{1a} \wedge Pr_{1b} \wedge \neg Co$, donde ser-0111 denota un ser que no hace lo que tú dices, que hace lo que yo digo, que hace trampas y que es un robot:

  Pr_{0a}: Cualquier ser-0111 hace lo que tú dices o lo que yo digo, (V)

  aunque

  Pr_{0b}: hay algún ser-0111 que hace trampas que no hace lo que tú dices. (V)

  Sin embargo,

  Pr_{1a}: los seres-0111 que hacen lo que tú dices y los seres-0111 que son robots hacen lo que yo digo, (V)

  y además,

  Pr_{1b}: los seres-0111 que hacen trampas, hacen lo que yo digo. (V)

  En fin, que

  Co: es falso que los seres-0111 que hacen lo que tú dices, hacen lo que yo digo. (F)

- Por otro, el contramodelo I_{0110} también lo permite, ya que el hecho de que exista un ser no robot tramposo que haga lo que yo digo pero que no haga lo que tú dices, es suficiente para que se satisfagan las premisas y no se satisfaga la conclusión, ya que es precisamente un contraejemplo a lo que se afirma en ella; de hecho, una contraargumentación es $Pr_{0a} \wedge Pr_{0b} \wedge Pr_{1a} \wedge Pr_{1b} \wedge \neg Co$, donde ser-0110 denota un ser que no hace lo que tú dices, que hace lo que yo digo, que hace trampas y que no es un robot:

  Pr_{0a}: Cualquier ser-0110 hace lo que tú dices o lo que yo digo, (V)

  aunque

  Pr_{0b}: hay algún ser-0110 que hace trampas que no hace lo que tú dices. (V)

Sin embargo,

Pr_{1a}: los seres-0110 que hacen lo que tú dices y los seres-0110 que son robots hacen lo que yo digo, (V)

y además,

Pr_{1b}: los seres-0110 que hacen trampas, hacen lo que yo digo. (V)

En fin, que

Co: es falso que los seres-0110 que hacen lo que tú dices, hacen lo que yo digo. (F)

B. **Estrategia 1. Tablas de verdad.**

0. *Identificación de los contramodelos para A generados.*

   La tabla de verdad para A proporciona dos contramodelos para la forma lógica A, a saber, los mismos que proporcionó la expresión en FNC de A, I_{0111} e I_{0110}.

1. *Demostración de que los contramodelos lo son para A.*

   Vid. apartado 2.A.1.

2. *Expresión en español de las contraargumentaciones proporcionadas por los contramodelos.*

   Vid. apartado 2.A.2. ■

§ 10.19 Bibliografía

- Para una primera aproximación:

[145] José García García y Manuel López Pellicer. *Álgebra lineal y geometría: curso teórico-práctico*. Marfil, Alcoy, Hoya de Alcoy, Alicante (ES-A), España, 8.ª ed., 1992.

[146] Armando Óscar Rojo. *Álgebra I*. El Ateneo, Buenos Aires (AR-C), Argentina, 1986. ©TDR.

- Para estudiar, practicar y saber más:

[147] Herbert Bruce Enderton. *Elements of Set Theory*. Academic Press, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1977.

[148] Karel Hrbacek y Thomas J. Jech. *Introduction to set theory*. Monographs and textbooks in pure and applied mathematics. Marcel Dekker, Nueva York, Nueva York (US-NY), Estados Unidos de América, 3.ª ed., 1999.

[149] Józef Maria Bocheński. *Compendio de lógica matemática*. Colección Lógica y Teoría de la Ciencia. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1982. Traducido del inglés *A Précis of Mathematical Logic* (1959), traducido a su vez de *Précis de logique mathématique* (1948), Bussum, North Holland: F. G. Kroonder.

- Y más:

[64] Manuel Garrido Giménez. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989).

[140] Máximo Anzola González y José Ramón Caruncho Castro. *Problemas de álgebra. Tomo 1: Conjuntos - Grupos*. Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1981. ©TDR.

[141] John Kenneth Truss. *Discrete mathematics for computer scientists*. Addison-Wesley, Bungay, Suffolk (GB-SFK), Reino Unido, 1991.

[144] Agustín de la Villa Cuenca. *Problemas de Álgebra (con esquemas teóricos)*. CLAGSA, Madrid, Comunidad de Madrid (ES-M), España, 4.ª ed., 2010. ©TDR.

- Para profundizar, acullá:

[142] José Antonio Alonso Jiménez, Joaquín Borrego Díaz, Mario de Jesús Pérez Jiménez y José Luis Ruiz Reina. *Curso Práctico de Teoría de Conjuntos*. La Ñ, Sevilla, Andalucía (ES-AN), España, 1998.

- Sin olvidar a los recomendados dedicados a la matemática discreta:

[32] Félix García Merayo. *Matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 2015.

[141] John Kenneth Truss. *Discrete mathematics for computer scientists*. Addison-Wesley, Bungay, Suffolk (GB-SFK), Reino Unido, 1991.

[150] Félix García Merayo, Gregorio Hernández Peñalver y Antonio Nevot Luna. *Problemas resueltos de matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 2018.

[151] Kenneth Howard Rosen. *Matemática discreta y sus aplicaciones*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 5.ª ed., 2004. (La 5.ª edición es la última en español).

[152] Kenneth Howard Rosen. *Discrete Mathematics and its Applications*. McGraw-Hill, Nueva York, Nueva York (US-NY), Estados Unidos de América, 7.ª ed., 2012.

[153] Francisco José González Gutiérrez. *Apuntes de Matemática Discreta*. El autor, Cádiz, Andalucía (ES-AN), España, 2004.

[154] Carlos GARCÍA GÓMEZ, Josep María LÓPEZ BESORA y Dolors PUIGJANER RIBA. *Matemática discreta*. Pearson Educación, Madrid, Comunidad de Madrid (ES-M), España, 2002.

[155] Ralph Peter GRIMALDI. *Matemáticas discreta y combinatoria*. Addison-Wesley Iberoamericana, Wilmington, New Castle, Delaware (US-DE), Estados Unidos de América, 3.ª ed., 1997.

[124] Jiří MATOUŠEK y Jaroslav NEŠETŘIL. *Invitación a la matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2008.

[156] Juan Carlos FERRANDO PÉREZ y Valentín GREGORI GREGORI. *Matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2.ª ed., 2012.

[157] Kenneth Allen ROSS y Charles Richard Bowers WRIGHT. *Matemáticas discretas*. Prentice-Hall Hispanoamericana, Naucalpan de Juárez, Estado Libre y Soberano de México (MX-MEX), Estados Unidos Mexicanos, 2.ª ed., 1990.

[158] Richard JOHNSONBAUGH. *Discrete Mathematics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 8.ª ed., 2018.

Capítulo 11

Lógica de relaciones

Jamás ha habido criaturas; sólamente ha habido parejas.

(Jean Giraudoux, *Sodoma y Gomorra*).

Un autor humorístico ha dicho que la humanidad entera podía dividirse en tres grandes grupos: oficiales, asistentes y deshollinadores. Esta ocurrencia no me parece a mí un puro chiste, sino que la juzgo muy significativa y profunda, de suerte que se necesita un talento especulativo muy grande para poder superar esa división con otra mejor. Porque cuando una división o clasificación no agota idealmente su objeto, entonces lo mejor es sustituirla por otra completamente arbitraria y accidental, pues ésta, al menos, tiene la ventaja de poner la imaginación en movimiento. Una clasificación aproximada no puede satisfacer a la razón y, por otra parte, no le dice absolutamente nada a la fantasía. Por eso es preferible rechazarla de plano y cuanto antes, a pesar de que en el uso corriente goce de la mayor estima, gracias a la enorme necedad de los humanos y a su carencia casi completa de imaginación.

(Søren Aabye Kierkegaard , 1813–1855, *La repetición*, 1843).

Otto Neugebauer le refirió al autor la siguiente leyenda acerca de Einstein. Parece ser que Einstein fue un niño tardo en hablar, lo cual, naturalmente, tenía preocupados a sus padres. Finalmente, un día, durante la cena, rompió a hablar, con la siguiente frase: «Die Suppe ist zu heiss» (La sopa está demasiado caliente). Sus padres se sintieron muy aliviados, pero enseguida le preguntaron por qué no había hablado hasta entonces. He aquí su respuesta: «Bisher war Alles in Ordnung» (Hasta ahora todo estuvo en orden).

(Philip J. Davis y Reuben Hersh, *Experiencia matemática*. MEC-Labor, Barcelona, 1989, pág. 132).

Mas que yo, criado en regalo, de padres políticos y curiosos, no sintiese tal engaño, grande fue mi hambre y esta escusa me desculpa. El deseo de comer algo bueno era grande: todo se les hizo a mis ojos pequeño. El traidor del mesonero lo daba destilado: no es maravilla; cuando tuviera defectos mayores, me pareciera banquete formado. ¿No has oído decir que a la hambre no hay mal pan? Digo que se me hizo almíbar y me dejó goloso.

(Mateo Alemán, *Primera parte del Guzmán de Alfarache*, 1599, Cátedra: 1992, pág. 192).

Ande yo caliente, y ríase la gente.

(Refrán).

Ya presentadas por Aristóteles en sus *Tópicos*, será Peirce quien define la relación como clase de pares, visión que completan Frege y Peano y cuya formalización se plasma en los *Principia Mathematica* de Russell y Whitehead (1910-1913). Durante el siglo XX se cuida y desarrolla su teoría y práctica —Wiener (1912/14), Kuratowski (1921), Quine (1951)—. Diseñar, analizar e interpretar árboles, grafos y redes es impensable sin un conocimiento de la teoría de las relaciones. A la hora de estudiar las redes sociales, por ejemplo, la programación lógico-matemática-computacional orientada a las relaciones propiamente y no a ellas como entidades (objetos) se hace imprescindible.

Como humanos, es frecuente que la asociación entre conceptos prime sobre la estructuración de la información, por lo que el conocimiento se adquiera a través de las relaciones existentes entre los conceptos y las propiedades y peculiaridades que los caracterizan.

Las clasificaciones y ordenaciones son básicas para nuestros actos de decisión o juicios por comparación, así que no está de más comenzar por una visión general de las relaciones y el estudio de las relaciones funcionales como preliminar al de las funciones con dos ejemplos de familias, la de los conjuntos de palabras de la misma longitud y la partición de un conjunto. Sigue a todo ello el estudio de las propiedades de más frecuente aparición de las relaciones diádicas —*cfr.* §11.0—. A renglón seguido, nos pareció oportuno centrarnos en los órdenes —*cfr.* §11.26—, debido principalmente a que las decisiones que tomemos en nuestros actos de elección, base de la discusión central de muchas de estas páginas, son decisiones de orden: es posible que elijamos una entidad entre varias, porque es admisible ordenarlas de acuerdo a nuestras preferencias (diremos que conseguimos definir una estructura de preferencias en la colección de entidades).

§ 11.0 Relaciones diádicas

Definición 11.0.— Definimos una *relación diádica* como

- un predicado diádico R, o como
- una subclase R de un producto cartesiano de clases $X \times Y$, o como
- un subconjunto R de un producto cartesiano de conjuntos $X \times Y$, o como
- una correspondencia $R : X \longrightarrow Y$ entre clases o conjuntos.

En este capítulo nos centramos en las vistas como subconjunto de un producto cartesiano y como correspondencia. En particular, R como subconjunto de $X \times Y$ significa que R es un conjunto de pares ordenados. Cuando $\langle x, y\rangle \in R$ decimos que «x está relacionado con y» y escribimos xRy (notación infijo) o Rxy (notación prefijo, justo tal y como se escribe considerando R como predicado diádico); decimos de x que es el *antecedente* de R y de y que es el *consecuente* de R; decimos *término* de R en vez de antecedente o consecuente de R.

Definición 11.1.— Dados dos conjuntos X e Y y una relación diádica $R \subseteq X \times Y$, entonces llamamos:

- *conjunto de partida* (o, sinónimamente, *conjunto inicial*) de R al conjunto X;
- *conjunto de llegada* (o, sinónimamente, *conjunto final*) de R al conjunto Y;
- *conjunto original* (o, sinónimamente, *conjunto de originales*, *conjunto de orígenes*, *dominio* o *imagen conversa*) de R al conjunto $\operatorname{dom} R = \{x \in X : \exists y \in Y, \langle x, y\rangle \in R\}$;
- *conjunto imagen* (o, sinónimamente, *imagen*, *conjunto de imágenes*, *contradominio*, *dominio converso*, *rango* o *recorrido*) de R al conjunto $\operatorname{ran} R = \{y \in Y : \exists x \in X, \langle x, y\rangle \in R\}$;
- *campo* de R al conjunto $\operatorname{cam} R = \operatorname{dom} R \cup \operatorname{ran} R$;
- *grafo* de R a la propia relación vista como conjunto, es decir, al conjunto $\{\langle x, y\rangle : xRy\}$ que designamos por la misma R, o, sinónimamente, por G_R, si queremos destacar que una relación R queda determinada cuando se conoce la terna (X, Y, G_R).

Observemos que, por definición, $R \subseteq \operatorname{dom} R \times \operatorname{ran} R$.

Teorema 11.0

Se satisface:

0. $\operatorname{cam} R = \operatorname{dom} R \leftrightarrow \operatorname{ran} R \subseteq \operatorname{dom} R$,
1. $\operatorname{cam} R = \operatorname{ran} R \leftrightarrow \operatorname{dom} R \subseteq \operatorname{ran} R$.

Definición 11.2.— La *relación nula* $\emptyset$ es aquélla cuyo campo es el conjunto vacío, esto es, $\emptyset = \{\langle x, y\rangle : x \neq x \wedge y \neq y\}$.

En el sentido de la inclusión conjuntista no hay relación menor que la relación nula: nada, absolutamente nada está relacionado.

Definición 11.3.— La relación $X \times Y = \{\langle x, y\rangle : x \in X \wedge y \in Y\}$ es la *relación total* en $X \times Y$.

En el sentido de la inclusión de conjuntos y siendo el referencial $X \times Y$, la relación total es la mayor.

De cualquier relación que sea distinta de la relación nula $\emptyset$ y de la relación total $X \times Y$ decimos que es una *relación propia* en $X \times Y$.

Definición 11.4.— La relación $\mathcal{U} = \{\langle x, y\rangle : x = x \wedge y = y\}$ es la *relación universal*.

En el sentido de la inclusión conjuntista no hay relación mayor que la relación universal: todo, absolutamente todo, está relacionado.

Si los conjuntos X e Y son iguales solemos decir que es una *relación homogénea* (o, sinónimamente, *endorrelación*), mientras que si son distintos hablamos de *relación heterogénea*.

Definición 11.5.— Llamamos *relación identidad* en X a la endorrelación $I_X = \{\langle x, x\rangle : x \in X\}$.

Observación 11.0.0.— En algunos textos, la relación identidad aparece designada por Δ y denominada *relación diagonal*.

Definición 11.6.— Dados dos conjuntos X e Y, una relación diádica $R \subseteq X \times Y$ y dos elementos relacionados xRy, decimos que

- x es *original del elemento* y de Y por R, y que
- y es *imagen del elemento* x de X por R,

por estar definida xRy como el par ordenado $\langle x, y\rangle$ y leerse el par de izquierda a derecha.

Observación 11.0.1.— Se lee de izquierda a derecha debido al orden inducido por la propia definición constructiva, $\langle x, y\rangle = \{\{x\}, \{x, y\}\}$, primero $\{x\}$, después $\{x, y\}$.

Análogamente definimos el origen de un subconjunto de Y y la imagen de un subconjunto de X.

Definición 11.7.— Dados dos conjuntos X e Y, $V \subseteq Y$ y una relación diádica $R \subseteq X \times Y$, el *origen del subconjunto* V de Y por R es

$$\mathrm{orig}_R V = \{x \in X : \exists y \in V, \langle x, y\rangle \in R\},$$

Observación 11.0.2.— El conjunto —$\mathrm{orig}_R V$ no es otro que la *imagen inversa del subconjunto* V, $\mathrm{im}_{R^{-1}} V$, una vez definida la relación inversa —*vid. infra* definición 11.10 (pág. 599 de esta edición)—.

Definición 11.8.— Dados dos conjuntos X e Y, $U \subseteq X$ y una relación diádica $R \subseteq X \times Y$, la *imagen del subconjunto* U de X por R es

$$\mathrm{im}_R U = \{y \in Y : \exists x \in U, \langle x, y\rangle \in R\},$$

siendo también notaciones habituales $R(U)$, $[U]_R$ o $\overline{U}^R$.

§ 11.1 Representaciones cartesiana, sagitaria, matricial, gráfica bipartita dirigida y digráfica

Sean $X = \{x_0, x_1, x_2, x_3\}$ e $Y = \{y_0, y_1, y_2, y_3\}$ y la relación diádica $R = \{\langle x_0, y_2\rangle, \langle x_0, y_3\rangle, \langle x_1, y_1\rangle, \langle x_2, y_0\rangle, \langle x_2, y_1\rangle, \langle x_3, y_0\rangle, \langle x_3, y_2\rangle, \langle x_3, y_3\rangle\}$. Destacamos otras cuatro representaciones.

Cartesiana, esto es, con ejes cartesianos.

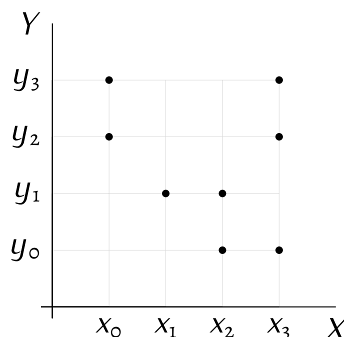


Figura 11.0.— Diagrama cartesiano de la relación diádica R.

Sagitaria, esto es, con conjuntos y flechas.

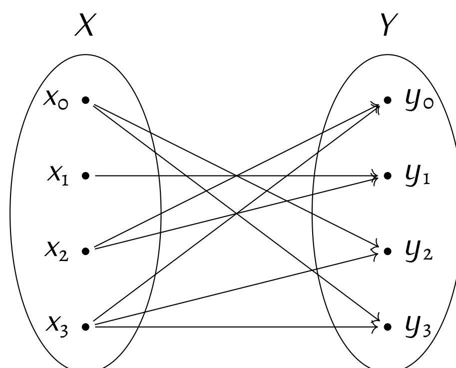


Figura 11.1.— Diagrama sagital de la relación diádica R.

Matricial, esto es, con una matriz lógica.

$$\begin{array}{c} \\ x_0 \\ x_1 \\ x_2 \\ x_3 \end{array} \begin{array}{c} \begin{array}{cccc} y_0 & y_1 & y_2 & y_3 \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Figura 11.2.— Matriz lógica de la relación diádica R.

Gráfica bipartita dirigida, esto es, mediante un grafo bipartito dirigido[○].

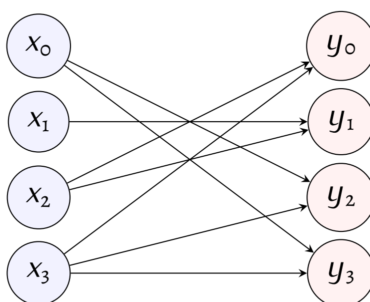


Figura 11.3.— Grafo bipartito dirigido de la relación diádica R.

Digráfica, esto es, mediante un grafo dirigido[1]. Suponiendo $X = Y$, elemento a elemento (es decir, siendo $x_0 = y_0, \ldots, x_3 = y_3$), tenemos también la siguiente representación como grafo dirigido (digrafo), DG_R.

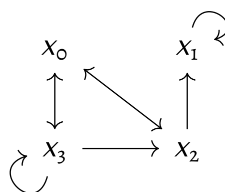


Figura 11.4.— Grafo dirigido (*digrafo*) de la relación diádica R.

Representamos este digrafo por el par ordenado $\langle K, A\rangle$, donde $K = \{x_0, x_1, x_2, x_3\}$ es el conjunto de *nodos/vértices* y $A \subseteq K \times K$, $A = \{\langle x_0, x_2\rangle, \langle x_0, x_3\rangle, \langle x_1, x_1\rangle, \langle x_2, x_0\rangle, \langle x_2, x_1\rangle, \langle x_3, x_0\rangle, \langle x_3, x_2\rangle, \langle x_3, x_3\rangle\}$, el conjunto de arcos —en los digrafos, dos nodos, digamos x e y, pueden estar unidos mediante un *arco*, hecho que representamos mediante el par ordenado $\langle x, y\rangle$, en cuyo caso llamamos *origen* del arco a x y *extremo* del arco a y; llamamos *lazo* a un arco del tipo $\langle x, x\rangle$, esto es, con origen y extremo iguales—.

Observación 11.1.0.— Por cierto, a partir del concepto de grafo dirigido es posible definir el de árbol[2]. Dados $x, y \in K$, llamamos *camino* de origen x y extremo y y notamos $c(x, y)$, precisamente si existe una sucesión de arcos, $\langle x_0, x_1\rangle$, $\langle x_1, x_2\rangle$, $\langle x_2, x_3\rangle$, ..., $\langle x_{n-1}, x_n\rangle$ tal que el extremo de un arco es el origen del siguiente y tal que $x_0 = x$ y $x_n = y$. Decimos que $x \in K$ es un *nodo terminal* precisamente si $\Gamma(x) = \emptyset$. Decimos que $o \in K$ es un *nodo distinguido* precisamente si no existe $x \in K$ tal que $o \in \Gamma(x)$. Dados $x, y \in K$, decimos que y es un *nodo posterior* a x precisamente si existe un camino $c(x, y)$. Un grafo es un *árbol* precisamente si se satisface: 0.°, $\forall x \in K$, $x \notin \Gamma(x)$, esto es, no existen lazos en el grafo; 1.°, existe un único nodo distinguido $o \in K$; 2.°, $\forall x \in K$, con $x \neq o$, x es posterior a o, y 3.°, $\forall x, y \in K$, con $x \neq y$, $\Gamma(x) \cap \Gamma(y) = \emptyset$.

○ *Cfr. supra* § 8.8 (p. xciii de esta edición).
1 *Cfr. supra* § 8.5 (p. lxxxix de esta edición).
2 Ya hemos hablado de árboles en § 9.0 (pág. xcv de esta edición).

Observación 11.1.1.— Representaciones alternativas son la *matriz de incidencia*, la *matriz de adyacencia* y la *lista de adyacencia*.

§ 11.2 El álgebra de Boole de las relaciones diádicas

Como tales conjuntos que son, por ser subconjuntos de un producto cartesiano, si R y S son relaciones definidas en $X \times Y$, también lo son las correspondientes a los conjuntos complementario, intersección, unión, diferencia y diferencia simétrica, esto es, se tienen: la *relación complementaria*, la *relación intersección* (llamada, a veces, *relación producto*), la *relación unión* (llamada, a veces, *relación suma lógica*), la *relación diferencia* y la *relación diferencia simétrica*, las cuales están definidas, $\forall \langle x, y\rangle \in X \times Y$ por:

$$\begin{aligned} R^{\complement} &\risingdotseq \{\langle x, y\rangle : \langle x, y\rangle \notin R\}; \\ R \cap S &\risingdotseq \{\langle x, y\rangle : \langle x, y\rangle \in R \wedge \langle x, y\rangle \in S\}; \\ R \cup S &\risingdotseq \{\langle x, y\rangle : \langle x, y\rangle \in R \vee \langle x, y\rangle \in S\}; \\ R \setminus S &\risingdotseq R \cap S^{\complement} \\ &:= \{\langle x, y\rangle : \langle x, y\rangle \in R \wedge \langle x, y\rangle \notin S\}; \\ R \Delta S &\risingdotseq (R \setminus S) \cup (S \setminus R) \\ &:= \{\langle x, y\rangle \in R : \langle x, y\rangle \notin S\} \cup \{\langle x, y\rangle \in S : \langle x, y\rangle \notin R\}. \end{aligned}$$

Estas intersecciones y uniones pueden extenderse a cualquier colección C no vacía de relaciones:

$$\begin{aligned} \bigcap C &\risingdotseq \{\langle x, y\rangle : \forall R \in C, \langle x, y\rangle \in R\}; \\ \bigcup C &\risingdotseq \{\langle x, y\rangle : \exists R \in C, \langle x, y\rangle \in R\}. \end{aligned}$$

Además, trabajamos con la inclusión, igualdad y exclusión de relaciones:

$$\begin{aligned} R \subseteq S &\risingdotseq \forall x \forall y (xRy \to xSy); \\ R = S &\risingdotseq \forall x \forall y (xRy \leftrightarrow xSy); \\ R \,||\, S &\risingdotseq \forall x \forall y (xRy \mid xSy). \end{aligned}$$

Teorema 11.1

Sean X un conjunto y 2^{X^2} el conjunto de todas las (endor)relaciones diádicas en X. Se satisface que la cuaterna $(2^{X^2}; \cap, \cup, {}^{\complement})$ es un *álgebra de* Boole.

Actividad 11.0

Representemos diagramáticamente con diagramas conjuntistas (no lógicos) de VENN la relación de igualdad según la traducción de la regla semántica de verdad de la equivalencia.

[Cubit 54].

§ 11.3 Matrices lógicas y digrafos de las relaciones entre relaciones

- Relación complementaria, $R^{\complement}$:
  - *matriz lógica*: los unos de $M_{R^{\complement}}$ son los ceros de M_R y los ceros de $M_{R^{\complement}}$ son los unos de M_R, esto es, $m_{ij}^{R^{\complement}} = \neg m_{ij}^{R}$;
  - *digrafo*: $DG_{R^{\complement}}$ tiene sólo las aristas que no tiene DG_R.
- Relación intersección, $R \cap S$:
  - *matriz lógica*: los unos de $M_{R\cap S}$ son los unos coincidentes de M_R y M_S y el resto son ceros, esto es, $m_{ij}^{R\cap S} = m_{ij}^{R} \wedge m_{ij}^{S}$;
  - *digrafo*: $DG_{R\cap S}$ tiene sólo las aristas que tienen simultáneamente DG_R y DG_S.
- Relación unión, $R \cup S$:
  - *matriz lógica*: los unos de $M_{R\cup S}$ son los unos de M_R y los unos de M_S, y sólo ésos, el resto son ceros, esto es, $m_{ij}^{R\cup S} = m_{ij}^{R} \vee m_{ij}^{S}$;
  - *digrafo*: $DG_{R\cup S}$ tiene todas las aristas que tiene DG_R y todas las que tiene DG_S, y sólo ésas.
- Relación diferencia, $R \setminus S$:
  - *matriz lógica*: los unos de $M_{R\setminus S}$ son los unos de M_R quitando los unos de M_S, esto es, $m_{ij}^{R\setminus S} = m_{ij}^{R} \wedge \neg m_{ij}^{S}$;
  - *digrafo*: $DG_{R\setminus S}$ es el digrafo de R del que se suprimen las aristas del digrafo de $R \cap S$.
- Relación diferencia simétrica, $R \Delta S$:
  - *matriz lógica*: los unos de $M_{R\Delta S}$ son los unos de $M_{R\cup S}$ quitando los unos de $M_{R\cap S}$, esto es, $m_{ij}^{R\Delta S} = m_{ij}^{R} \veebar m_{ij}^{S}$;
  - *digrafo*: $DG_{R\Delta S}$ es el digrafo de $R \cup S$ del que se suprimen las aristas del digrafo de $R \cap S$.

§ 11.4 Relación inversa

Definición 11.9.— Sean X y Y conjuntos y $R \subseteq X \times Y$ una relación. Llamamos *relación inversa* de R a

$$R^{-1} = \{\langle y, x\rangle \in Y \times X : \langle x, y\rangle \in R\}.$$

La relación inversa de R también es conocida como su *relación recíproca*, *conversa*, *transpuesta*, *opuesta* o *dual*.

Notemos que el conjunto inicial de R^{-1} es el conjunto final de R y que el conjunto final de R^{-1} es el conjunto inicial de R.

Con respecto a su matriz lógica y digrafo, tenemos:

- *matriz lógica* de R^{-1}: $M_{R^{-1}}$ es la transpuesta de M_R, esto es, $m_{ij}^{R^{-1}} = m_{ji}^{R}$;
- *digrafo* de R^{-1}: $DG_{R^{-1}}$ tiene las mismas aristas que el de DG_R pero dirigidas en sentido contrario;

Definición 11.10.— Sean dos conjuntos X y Y, una relación diádica $R \subseteq X \times Y$ y $C \subseteq Y$, entonces, llamamos *imagen inversa* (o, sinónimamente, *contraimagen*) de C por R a

$$\mathrm{im}_{R^{-1}} C = \{x \in X : \exists y \in C, \langle x, y\rangle \in R\}.$$

Observación 11.4.0.— El conjunto $\mathrm{im}_{R^{-1}} C$ no es otro que $\mathrm{orig}_R C$, esto es, el conjunto origen de C por R.[3]

Observación 11.4.1.— También son designaciones habituales,

- para la relación inversa de R: $\breve{R}$, $\widetilde{R}$, $R^{\top}$, $\mathrm{Inv}R$, $\mathrm{Cnv}R$, y
- para la imagen inversa de C por R: $R^{-1}(C)$, $[C]_{R^{-1}}$, $\overline{C}^{R^{-1}}$.

Veamos ahora algunas propiedades que son ejemplos de interrelación entre una relación y su inversa mediando incluso operaciones.

[3] *Cfr. supra* ejemplo 11.7 (pág. 594 de esta edición).

Teorema 11.2

Se satisface:

0. dom $R^{-1} = \operatorname{ran} R$;
1. ran $R^{-1} = \operatorname{dom} R$;
2. cam $R^{-1} = \operatorname{cam} R$;
3. cam $R = \operatorname{cam}(R \cup R^{-1})$.

Teorema 11.3

Se satisface:

4. $(R^{-1})^{-1} = R$;
5. $(S \cup R)^{-1} = R^{-1} \cup S^{-1}$;
6. $(S \cap R)^{-1} = R^{-1} \cap S^{-1}$;
7. $R \subseteq S^{-1} \leftrightarrow R^{-1} \subseteq S$;
8. $R = S^{-1} \leftrightarrow R^{-1} = S$;
9. $R = S \leftrightarrow R^{-1} = S^{-1}$;
10. $\exists! R^{-1}$;
11. $(R^{\complement})^{-1} = (R^{-1})^{\complement}$ (a veces, esta relación se denomina *relación dual* de R y se nota por R^{d});
12. $C \subseteq D \rightarrow \operatorname{im}_{R^{-1}} C \subseteq \operatorname{im}_{R^{-1}} D$.

Teorema 11.4

Si R es una proyección, entonces R^{-1} (la inversa o dual de R) es una asignación, y viceversa.

§ 11.5 Relación poliádica

Dados tres conjuntos X_0, X_1, X_2, una *relación triádica* es un subconjunto de ternas ordenadas definidas en la forma $\langle x_0, x_1, x_2 \rangle = \langle \langle x_0, x_1 \rangle, x_2 \rangle$; dados cuatro conjuntos X_0, X_1, X_2, X_3, una *relación tetrádica* es un subconjunto de cuaternas ordenadas definidas en la forma $\langle x_0, x_1, x_2, x_3 \rangle = \langle \langle x_0, x_1, x_2 \rangle, x_3 \rangle$; en general, dados n conjuntos $X_0, X_1, \ldots, X_{n-1}$, una *relación poliádica* de n argumentos/términos (o, sinónimamente, *relación enádica* o n-ádica)[4] es un subconjunto del producto cartesiano $X_0 \times X_1 \times \ldots \times X_{n-1}$, esto es, un subconjunto de tuplas enádicas ($n \in \mathbb{N}_{\geq 2}$) definidas en la forma[5] $\langle x_0, x_1, \ldots, x_{n-1} \rangle = \langle \langle x_0, x_1, \ldots, x_{n-2} \rangle, x_{n-1} \rangle$.

[4] También reciben el nombre de relaciones *binarias*, *ternarias*, *cuaternarias*, ..., *enarias*, pero prefiero las denominaciones *diádicas*, *triádicas*, etc., que empleamos y la razón es su significado (DRAE): «diádico, ca: perteneciente o relativo a la díada», «díada: pareja de dos seres o cosas *estrecha y especialmente vinculados entre sí*.», «binario, ria: compuesto de dos elementos, unidades o guarismos». Así, pudiésemos decir que un conjunto de dos elementos es un conjunto binario, aunque no entienda el porqué de la inconsistencia de llamar binaria y no diádica a una estrella doble.

[5] *Vid. supra* § 10.15 para conocer la razón de definir así las tuplas.

Es posible extender las definiciones anteriores vistas para relaciones diádicas a relaciones poliádicas n términos; por ejemplo, la *relación identidad* y la *imagen de un subconjunto* $S \subseteq X_0 \times X_1 \times \ldots \times X_{n-2}$ por R:

$$\begin{aligned} I_X &\coloneqq \{\langle x, x, \ldots, x\rangle : x \in X\}; \\ \mathrm{im}_R S &\coloneqq \{y \in X_{n-1} : \exists\langle x_0, x_1, \ldots, x_{n-2}\rangle \in S, \langle x_0, x_1, \ldots, x_{n-2}, y\rangle \in R\}. \end{aligned}$$

Este concepto de relación poliádica se generaliza para productos cartesianos de productos cartesianos (teniendo en cuenta su no asociatividad). Por ejemplo, dado un conjunto X, se define una endorrelación enádica R como un subconjunto de algún producto cartesiano $X^i \times X^j$, siendo $i, j \in \mathbb{Z}^+$ tales que $i + j = n$. Definimos entonces la imagen de un subconjunto $S \subseteq X^i$,

$$\begin{aligned} \mathrm{im}_R S = \{\langle x_i, x_{i+1}, \ldots, x_{i+j-1}\rangle \in X^j :& \exists\langle x_0, x_1, \ldots, x_{i-1}\rangle \in S, \\ & \text{tal que } \langle x_0, x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{i+j-1}\rangle \in R\}. \end{aligned} \tag{11.0}$$

En el caso de una relación poliádica de n términos se distinguen n *dominios*,

$$\operatorname*{dom}_k R \coloneqq \{x_k \in X_k : \exists\langle x_0, x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_{n-1}\rangle \in \prod_{i \in I} X_i, \langle x_0, x_1, \ldots, x_{n-1}\rangle \in R\}, \tag{11.1}$$

con $I = \{0, 1, \ldots, k-1, k+1, \ldots, n-1\}$;

Notamos por $R \upharpoonright_k D$ a la *relación limitada en su imagen* al conjunto $D \subseteq X_k$, esto es,

$$R \upharpoonright_k D \coloneqq \{\langle x_0, x_1, \ldots, x_{n-1}\rangle \in R : x_k \in D\}. \tag{11.2}$$

Notamos por $R \wr C$ a la *relación limitada en su campo* al conjunto C, o sea,

$$R \wr C \coloneqq C \upharpoonleft R \upharpoonright C \coloneqq \{\langle x_0, x_1, \ldots, x_{n-1}\rangle \in R : x_0, x_1, \ldots, x_{n-1} \in C\}. \tag{11.3}$$

Los conceptos de *relación complementaria* y de *intersección, unión, diferencia y diferencia simérica de relaciones* se generalizan para el caso de relaciones poliádicas; así, $\forall\langle x_0, x_1, \ldots, x_{n-1}\rangle \in X^n$:

$$\begin{aligned} R^{\complement} &\coloneqq \{\langle x_0, x_1, \ldots, x_{n-1}\rangle : \langle x_0, x_1, \ldots, x_{n-1}\rangle \notin R\}; \\ R \cap S &\coloneqq \{\langle x_0, x_1, \ldots, x_{n-1}\rangle : \langle x_0, x_1, \ldots, x_{n-1}\rangle \in R \wedge \langle x_0, x_1, \ldots, x_{n-1}\rangle \in S\}; \\ R \cup S &\coloneqq \{\langle x_0, x_1, \ldots, x_{n-1}\rangle : \langle x_0, x_1, \ldots, x_{n-1}\rangle \in R \vee \langle x_0, x_1, \ldots, x_{n-1}\rangle \in S\}; \\ R \setminus S &\coloneqq R \cap S^{\complement} \\ &\coloneqq \{\langle x_0, x_1, \ldots, x_{n-1}\rangle : \langle x_0, x_1, \ldots, x_{n-1}\rangle \in R \wedge \langle x_0, x_1, \ldots, x_{n-1}\rangle \notin S\}; \\ R \Delta S &\coloneqq (R \setminus S) \cup (S \setminus R) \\ &\coloneqq \{\langle x_0, x_1, \ldots, x_{n-1}\rangle \in R : \langle x_0, x_1, \ldots, x_{n-1}\rangle \notin S\} \\ &\quad \cup \{\langle x_0, x_1, \ldots, x_{n-1}\rangle \in S : \langle x_0, x_1, \ldots, x_{n-1}\rangle \notin R\}. \end{aligned}$$

Teorema 11.5
Una relación poliádica de n términos tiene $n! - 1$ relaciones inversas.

Ejemplo 311

¿Son cinco las inversas de la relación triádica $R \subseteq X \times Y \times Z$? ¿Cuáles?

Resolución.— En efecto, las $3! - 1 = 5$ inversas de la relación triádica $R \subseteq X \times Y \times Z$ son:

$$\begin{aligned}
R^{-1}_{\langle 1,3,2\rangle} &= \{\langle x,z,y\rangle \in X \times Z \times Y : \langle x,y,z\rangle \in R\}\\
R^{-1}_{\langle 2,1,3\rangle} &= \{\langle y,x,z\rangle \in Y \times X \times Z : \langle x,y,z\rangle \in R\}\\
R^{-1}_{\langle 2,3,1\rangle} &= \{\langle y,z,x\rangle \in Y \times Z \times X : \langle x,y,z\rangle \in R\}\\
R^{-1}_{\langle 3,1,2\rangle} &= \{\langle z,x,y\rangle \in Z \times X \times Y : \langle x,y,z\rangle \in R\}\\
R^{-1}_{\langle 3,2,1\rangle} &= \{\langle z,y,x\rangle \in Z \times Y \times X : \langle x,y,z\rangle \in R\}
\end{aligned}$$

Es posible representar las «flechas» de estas inversas como caminos dirigidos en el espacio tridimensional; así, si representamos la terna $\langle x,y,z\rangle \in R$ en los ejes XYZ, se tiene la biyección que muestra el siguiente cuadro.

Ternas	*Caminos dirigidos*
	Relación:
$\langle x,y,z\rangle = \langle\langle x,y\rangle,z\rangle \in R$	$\langle x,0,0\rangle, \langle x,y,0\rangle, \langle x,y,z\rangle$
	Inversas:
$\langle x,z,y\rangle = \langle\langle x,z\rangle,y\rangle$	$\langle x,0,0\rangle, \langle x,0,z\rangle, \langle x,y,z\rangle$
$\langle y,x,z\rangle = \langle\langle y,x\rangle,z\rangle$	$\langle 0,y,0\rangle, \langle x,y,0\rangle, \langle x,y,z\rangle$
$\langle y,z,x\rangle = \langle\langle y,z\rangle,x\rangle$	$\langle 0,y,0\rangle, \langle 0,y,z\rangle, \langle x,y,z\rangle$
$\langle z,x,y\rangle = \langle\langle z,x\rangle,y\rangle$	$\langle 0,0,z\rangle, \langle x,0,z\rangle, \langle x,y,z\rangle$
$\langle z,y,x\rangle = \langle\langle z,y\rangle,x\rangle$	$\langle 0,0,z\rangle, \langle 0,y,z\rangle, \langle x,y,z\rangle$ ■

Cuadro 11.0.— Propiedades frecuentemente satisfechas por una relación diádica R definida sobre un conjunto no vacío C.
—Fuente: Elaboración propia.

Para el cálculo de la *imagen inversa de un conjunto* hemos de saber dónde se sitúa dicho conjunto. Por ejemplo, para una relación triádica $R \subseteq X \times Y \times Z$, son de interés:

$$C \subseteq Y \times Z \to R^{-1}_{(y,z)}(C) = \{x \in X : \exists\langle y,z\rangle \in C,\ \langle x,y,z\rangle \in R\}, \tag{11.4}$$

$$C \subseteq Z \to R^{-1}_{(z)}(C) = \{\langle x,y\rangle \in X \times Y : \exists z \in C,\ \langle x,y,z\rangle \in R\}. \tag{11.5}$$

Una relación poliádica R con n términos incluye $C(n,k)$ subrelaciones de k términos, denominadas relaciones parciales o *proyecciones* de R, notadas $\Pi_U(R)$ donde U es el conjunto de términos que nos interesa saber cómo están relacionados según R.

Ejemplo 312

¿Cuántas proyecciones diádicas, triádicas, etc., incluye una relación pentádica $R(x,y,z,s,t)$?

Resolución.— Una relación pentádica $R(x,y,z,s,t)$ incluye:

- $\binom{5}{2} = 10$ proyecciones diádicas, a saber, $\Pi_{x,y}(R)$, $\Pi_{x,z}(R)$, $\Pi_{x,s}(R)$, $\Pi_{x,t}(R)$, $\Pi_{y,z}(R)$, $\Pi_{y,s}(R)$, $\Pi_{y,t}(R)$, $\Pi_{z,s}(R)$, $\Pi_{z,t}(R)$ y $\Pi_{s,t}(R)$;
- $\binom{5}{3} = 10$ proyecciones triádicas, a saber, $\Pi_{x,y,z}(R)$, $\Pi_{x,y,s}(R)$, $\Pi_{x,y,t}(R)$, $\Pi_{x,z,s}(R)$, $\Pi_{x,z,t}(R)$, $\Pi_{x,s,t}(R)$, $\Pi_{y,z,s}(R)$, $\Pi_{y,z,t}(R)$, $\Pi_{y,s,t}(R)$ y $\Pi_{z,s,t}(R)$;
- $\binom{5}{4} = 5$ proyecciones tetrádicas, a saber, $\Pi_{x,y,z,s}(R)$, $\Pi_{x,y,z,t}(R)$, $\Pi_{x,y,s,t}(R)$, $\Pi_{x,z,s,t}(R)$ y $\Pi_{y,z,s,t}(R)$), y
- $\binom{5}{5} = 1$ proyección pentádica, $\Pi_{x,y,z,s,t}(R) = R$. ■

Observación 11.5.0.— Con respecto a la representación gráfica de una relación triádica, tenemos su representación cartesiana añadiendo un tercer eje y su representación matricial como una matriz o tabla de tres dimensiones. Para relaciones poliádicas de más de tres argumentos, esta última.

§ 11.6 Relación composición

Definición 11.11.— Sean X, Y, U y V conjuntos y $R \subseteq X \times Y$ y $S \subseteq U \times V$ dos relaciones tales que $\mathrm{ran}(R) \subseteq \mathrm{dom}(S)$, entonces definimos la *relación composición* (que también llamamos *producto relacional*) de R y S por

$$S \circ R \coloneqq \{\langle x,z\rangle \in X \times V : (\exists y \in Y)(xRy \wedge ySz)\}.$$

Observación 11.6.0.— Aunque la notación $S \circ R$ invierte la secuencia de texto (S, después R) con respecto de la secuencia de actuación (R, después S), la utilizamos por similitud con la notación de composición de funciones $(g \circ f)(x) = g(f(x))$ —*cfr. infra* § 12.2 (pág. 694 de esta edición)— (*vid. qq. infra* la discusión de Jesús Mosterín al respecto —observación 11.19.0 (pág. 625 de esta edición)—).

Dos notaciones alternativas que no la invierten son: $R; S$ y $R|S$.

La *matriz lógica* de $S \circ R$, $M_{S \circ R}$ es $M_R \odot M_S$ (producto booleano), esto es,

$$m_{ij}^{S \circ R} \leftrightharpoons \bigvee_{k=0}^{n} \left(m_{ik}^{R} \wedge m_{kj}^{S} \right). \tag{11.6}$$

Definición 11.12.— Llamamos *relación potencia enésima* de R a $R^n \leftrightharpoons R \circ R^{n-1}$, siendo $R^0 = I_X$ y R una endorrelación diádica en un conjunto X.

Observación 11.6.1.— En caso de desconocer el conjunto X pudiésemos definir R^0 por $I \upharpoonright \operatorname{cam} R$, es decir, por $\{\langle x, y\rangle \in I : y \in \operatorname{cam} R\}$, en definitiva, por $\{\langle y, y\rangle : y \in \operatorname{cam} R\}$.

Ejemplo 313

Formalicemos «las amistades de nuestras amistades son nuestras amistades».

Resolución.— Si R es la relación «tener amistad con», entonces la frase anterior se formaliza como $R^2 \subseteq R$. ■

Teorema 11.6 (Peculiaridades y propiedades de la composición de relaciones)
Sean R, S y T tres relaciones que satisfacen los requisitos apropiados para las composiciones que aparecen a continuación, entonces:

0. $S \circ R \neq R \circ S$; (no conmutativa)
1. $S \circ R \subseteq \operatorname{dom}(R) \times \operatorname{ran}(S)$;
2. $(T \circ S) \circ R = T \circ (S \circ R)$; (asociativa)
3. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$. (inversa de la composición)

Con respecto a la relación de identidad se satisface lo establecido por el siguiente teorema.

Teorema 11.7
Sean X y Y conjuntos y $R \subseteq X \times Y$; se satisface:

0. $\operatorname{id}_{\operatorname{dom} R} \subseteq R^{-1} \circ R$;
1. $\operatorname{id}_{\operatorname{ran} R} \subseteq R \circ R^{-1}$.

Ejemplo 314

Visualizar el teorema anterior siendo $X = Y = \{a, b\}$, $R = \{\langle a, b\rangle\}$.

Resolución.— Tenemos entonces: $\operatorname{dom} R = \{a\}$, $\operatorname{ran} R = \{b\}$, $\operatorname{id}_{\operatorname{dom} R} = \{\langle a, a\rangle\}$, $\operatorname{id}_{\operatorname{ran} R} = \{\langle b, b\rangle\}$, $R^{-1} = \{\langle b, a\rangle\}$, $R^{-1} \circ R = \{\langle a, a\rangle\}$, $R \circ R^{-1} = \{\langle b, b\rangle\}$. ■

§ 11.7 Relación ancestral

Dada una relación R como norma definidora de la estructura o pauta de relación y dados unos hechos de relación, aRb, bRc, cRd, etc. (extensión concretizadora de R), definimos la relación R^*, «ser un ancestro (en la R-serie) de»

Definición 11.13.— Decimos que $C \subseteq \mathcal{U}$ es una *clase hereditaria* respecto de la relación R (sinónimamente, una clase R-hereditaria) precisamente si ocurre que

$$(\forall x, y \in \mathcal{U})(x \in C \wedge xRy \rightarrow y \in C), \tag{11.7}$$

lo que siendo $C = \{x \in \mathcal{U} : \phi x\}$ equivale a que

$$(\forall x, y \in \mathcal{U})(\phi x \wedge xRy \rightarrow \phi y). \tag{11.8}$$

Observación 11.7.0.— Alternativamente, C es una clase R-hereditaria si, y sólo si,

$$R^{-1}(C) \subseteq C, \tag{11.9}$$

por lo que la clase *Her* de todas las clases hereditarias es

$$\text{Her} = \{C \subseteq \mathcal{U} : (\exists R)(R^{-1}(C) \subseteq C)\}. \tag{11.10}$$

Ejemplo 315

En un árbol en el que los nodos corresponden a personas, representando la relación R «ser *ascendiente lindante* de», y siendo C la clase de las personas que hablan español, entonces si x es una persona de habla española y x es ascendiente lindante de y, lo habitual es que y, *descendiente lindante* de x, también hable español.

Definición 11.14.— Dada una relación R cualquiera, definimos dos nuevas relaciones, a partir del hecho de que u es un R-ascendiente de v precisamente si u tiene todas las propiedades que han heredado los R-descendientes de cualquier R-descendiente de v.

0. *Relación ancestral fuerte* (R^*): Consideramos que u es un R-ascendiente propio de v, esto es, que $u \neq v$, entonces,

$$vR^*u \leftrightharpoons (\forall C)((\forall x)(vRx \rightarrow x \in C) \wedge (\forall x, y)(x \in C \wedge xRy \rightarrow y \in C) \rightarrow u \in C)).$$

1. *Relación ancestral débil* ($R^{*=}$): Consideramos la posibilidad de ser $u = v$, entonces,

$$vR^{*=}u \leftrightharpoons (vR^*u) \vee (u = v)$$

$$\leftrightarrow (\forall C)(v \in C \wedge (\forall x, y)(x \in C \wedge xRy \to y \in C) \to u \in C)).$$

Observación 11.7.1.— Estas definiciones proceden de FREGE, vía BOOLOS [159] (pág. 286). Hemos de notar que BOCHEŃSKI [149] (pág. 92) denomina relación ancestral a la ancestral fuerte que nota R_*. En el libro de BOOLOS también encontramos cómo demostrar a partir de ambas relaciones los principios de inducción débil e inducción fuerte[6]. Notemos finalmente que las definiciones de estas relaciones no pertenecen a la lógica de primer orden sino a la de segundo orden[7] (usando las propiedades definitorias de las clases involucradas).

Ejemplo 316

Si R es la sucesión sucesor, ¿cuáles son R^* y $R^{*=}$?

Resolución.— Si R es la sucesión sucesor, entonces R^* es la clase de los números mayores que uno dado y $R^{*=}$ la de los números mayores o iguales a uno dado. ■

Teorema 11.8
La relación ancestral fuerte R^* es precisamente la clausura transitiva R^+ de R.

Demostración.— Demostremos que $R^+ = R^*$ por doble inclusión.

$\subseteq$: Se demuestra,

0. por un lado, que R^* es transitiva, lo cual no es complicado;

1. por otro, que $R \subseteq R^*$, ya que si xRy, entonces y satisface cualquier propiedad R-heredada que satisfaga cualquier entidad x tal que aRx pues y es una de tales entidades x;

es decir, R^* es una relación transitiva que incluye a R, por lo que incluye a R^+ por definición de clausura transitiva (R^+ es la menor relación transitiva que incluye a R), en definitiva, $R^+ \subseteq R^*$.

$\supseteq$: Supongamos que se satisface que vR^*u y fijémonos en una clase C particular, la clase de equivalencia de v por R^+, $C = [v]_{R^+} = \{x : vR^+x\}$ (es aceptable que nos fijemos en una clase particular, ya que según la definición de R^* —*vid. supra* definición 11.14.0 (pág. 605 de esta edición)— se satisface para cualquier clase C); pues bien, de la definición de R^* se deduce que $u \in C$, es decir, que $u \in [v]_{R^+}$, esto es, que vR^+u; en definitiva, $R^* \subseteq R^+$. ■

[6] *Cfr. infra* § 16.0 (pág. 805 de esta edición) y § 16.1 (pág. 810 de esta edición).
[7] *Vid. supra* pág. 372.

§ 11.8 Relación funcional

Reseñaremos más adelante el hecho de que las correspondencias, funciones, aplicaciones y operaciones son tipos particulares de relaciones —*cfr. infra* § 11.10 (pág. 611 de esta edición)—. Aprenderemos más sobre ellas en el capítulo 12 (pág. 690 de esta edición) y siguientes.

Definición 11.15 (Relaciones inyectivas, sobreyectivas y biyectivas).— Sean X e Y conjuntos y $R \subseteq X \times Y$ una relación. Entonces, decimos que:

0. R es *inyectiva* precisamente si todo elemento del rango tiene un único origen, es decir, si, y sólo si, es tal que
$$(\forall y \in \operatorname{ran} R)(\exists! x \in \operatorname{dom} R)(xRy),$$
lo que equivale a decir que es tal que
$$(\forall x, y \in \operatorname{dom} R)(\forall z \in \operatorname{ran} R)(xRz \land yRz \to x = y);$$

1. R es *sobreyectiva* (o, sinónimamente, *suprayectiva* o *exhaustiva*) precisamente si $\operatorname{ran} R = Y$, es decir, precisamente si todo elemento del conjunto final es imagen de algún elemento del dominio, esto es, si, y sólo si,
$$(\forall y \in Y)(\exists x \in \operatorname{dom} R)(xRy);$$

2. R es *biyectiva* precisamente si es inyectiva y sobreyectiva.

Teorema 11.9 (Caracterización de la biyectividad)
Sean X e Y conjuntos y $R \subseteq X \times Y$ una relación. Se satisface que R es biyectiva si, y sólo si,
$$(\forall y \in Y)(\exists! x \in \operatorname{dom} R)(xRy).$$

Actividad 11.1

Demostremos el teorema anterior.

Definición 11.16 (Relación funcional (o unívoca)).— Dados dos conjuntos X e Y, decimos que una relación $R \subseteq X \times Y$ es una *relación funcional* (o, sinónimamente, *relación unívoca*) de X en Y (o en $X \times Y$) precisamente si es tal que para cualquier $x \in \operatorname{dom} R$ existe como mucho un $y \in Y$ tal que xRy, es decir, si, y sólo si, todo elemento del dominio tiene una sola imagen, en definitiva, si, y sólo si,
$$(\forall x \in \operatorname{dom} R)(\forall y, z \in \operatorname{ran} R)(xRy \land xRz \to y = z).$$

En este caso decimos que X *determina funcionalmente* Y (o, sinónimamente, que Y *depende funcionalmente* de X).

Si $R \subseteq X \times X$, decimos que es funcional precisamente si $R^{-1} \circ R \subseteq \mathrm{id}_X$.

Ejemplo 317

0. La relación $\{\langle 0, 0\rangle, \langle 1, 2\rangle\}$ es funcional en $\mathbb{N}^2$.

1. La relación $\{\langle 0, 0\rangle, \langle 0, 1\rangle\}$ no es funcional en $\mathbb{N}^2$.

2. La relación $\{\langle m, n\rangle \in \mathbb{N}^2 : n = 2m\}$ es funcional en $\mathbb{N}^2$.

3. Dado un conjunto C, la relación $\{\langle X, Y\rangle \in 2^C \times 2^C : X \subseteq Y\}$, por lo general, no es funcional en 2^C, ya que un subconjunto puede serlo de varios conjuntos.

Teorema 11.10 (Composición de relaciones funcionales)
Sean X, Y, U y V conjuntos y $R \subseteq X \times Y$ y $S \subseteq U \times V$ dos relaciones tales que $\mathrm{ran}\, R \subseteq \mathrm{dom}\, S$, entonces la relación composición $S \circ R$ es una relación funcional en $X \times V$.

Definición 11.17.— Si R y R^{-1} son relaciones funcionales, decimos que R es una *relación bifuncional* (o, sinónimamente, *relación biunívoca* o *biyectiva parcial*).

Teorema 11.11 (Caracterización por funcionalidad de la inyectividad)
Sean X e Y conjuntos y $R \subseteq X \times Y$. Entonces,

R es inyectiva si, y sólo si, R^{-1} es funcional.

Teorema 11.12 (Caracterización por inyectividad de la bifuncionalidad)
Una relación es bifuncional si, y sólo si, es una relación funcional inyectiva.

Ejemplo 318

0. La relación $R = \{\langle 0, 0\rangle, \langle 1, 2\rangle\}$ es funcional —i. e., unívoca— e inyectiva en $\mathbb{N}^2$, i. e., por el teorema 11.12 (pág. 608 de esta edición), es una relación bifuncional —i. e., biunívoca— en $\mathbb{N}^2$ —observemos que $R^{-1} = \{\langle 0, 0\rangle, \langle 2, 1\rangle\}$ es funcional en $\mathbb{N}^2$ y que, por tanto, por el teorema 11.11 (pág. 608 de esta edición), R es inyectiva—.

1. La relación $R = \{\langle 0, 0\rangle, \langle 1, 0\rangle\}$ no es inyectiva en $\mathbb{N}^2$ —observemos que $R^{-1} = \{\langle 0, 0\rangle, \langle 0, 1\rangle\}$ no es funcional en $\mathbb{N}^2$ y que, por tanto, por el teorema 11.11 (pág. 608 de esta edición), R no es inyectiva—.

2. La relación $\{\langle m, n\rangle \in \mathbb{N}^2 : n = 2m\}$ es bifuncional en $\mathbb{N}^2$.

Ejemplo 319

Dado un conjunto X, la *relación de identidad* $I_X = \{\langle x, x\rangle : x \in X\}$ es funcional e inyectiva en X^2 —notemos respecto de lo último que $I_X^{-1} = I_X$ es funcional en X^2—.

Ejemplo 320

Dado un conjunto C, definimos la *relación de pertenencia* en C por $\in_C = \{\langle x, y\rangle \in C^2 : x \in y\}$. Sea $C = \{x, y, \{x\}, \{y\}, \{x, y\}\}$, ¿es la relación de pertenencia en C una relación funcional? ¿Es inyectiva?

Resolución.— Pues no, la relación de pertenencia en C no es ni funcional (pues $x \in \{x\} \wedge x \in \{x, y\}$) ni inyectiva (ya que $x \in \{x, y\} \wedge y \in \{x, y\}$), esto es, $\langle x, \{x\}\rangle$, $\langle x, \{x, y\}\rangle$, $\langle y, \{x, y\}\rangle$ son pares ordenados de tal relación en dicho conjunto. De hecho, $\in_C = \{\langle x, \{x\}\rangle, \langle x, \{x, y\}\rangle, \langle y, \{y\}\rangle, \langle y, \{x, y\}\rangle\}$; respecto de la no inyectividad, notemos que $\in_C^{-1} = \{\langle \{x\}, x\rangle, \langle \{x, y\}, x\rangle, \langle \{y\}, y\rangle, \langle \{x, y\}, y\rangle\}$ no es funcional. ■

§ 11.9 Restricción y extensión de una relación

Introducimos las nociones de relación con dominio limitado, imagen limitada y campo limitado.

Definición 11.18.— Sea R una relación diádica definida en un superconjunto de $X \times Y$.

0. $X \upharpoonleft R$ designa la *relación limitada en su dominio* al conjunto X, esto es,

$$X \upharpoonleft R = \{\langle x, y\rangle \in R : x \in X\};$$

1. $R \upharpoonright Y$ designa la *relación limitada en su imagen* al conjunto Y, es decir,

$$R \upharpoonright Y = \{\langle x, y\rangle \in R : y \in Y\};$$

2. $X \upharpoonleft R \upharpoonright Y$ designa la *relación limitada en su dominio* al conjunto X *y en su imagen* al conjunto Y, o sea,

$$X \upharpoonleft R \upharpoonright Y = \{\langle x, y\rangle \in R : x \in X \wedge y \in Y\};$$

3. $R \upharpoonleft X$ designa la *relación limitada en su campo* al conjunto X, a saber,

$$R \upharpoonleft X = X \upharpoonleft R \upharpoonright X = \{\langle x, y\rangle \in R : x, y \in X\}.$$

Observación 11.9.0.— Es costumbre notar $X \upharpoonleft R$ simplemente por $R|_X$ y decir de ella que es una *restricción* de R (a X) —y análogamente, decir de R que es una *extensión* de $R|_X$ (a algún superconjunto de X donde esté definida R)—.

Teorema 11.13 (Restricción y extensión de relaciones funcionales)

0. La restricción de una relación funcional es funcional.
1. La restricción de una relación inyectiva es inyectiva.
2. La extensión de una relación sobreyectiva es sobreyectiva.

Definición 11.19 (Relaciones uno/muchos a uno/muchos).— Distinguimos cuatro tipos.

0. Una *relación de uno a muchos*, notada $1 \to V$ (o, sinónimamente, $1 : N$), es una relación R restringida en su dominio a los subconjuntos unitarios, es decir, tal que

$$(\forall x, y \in \operatorname{dom} R)(\forall z \in \operatorname{ran} R)(xRz \wedge yRz \to x = y).$$

1. Una *relación muchos a uno*, notada $V \to 1$ (o, sinónimamente, $N : 1$), es una relación R restringida en su imagen a los subconjuntos unitarios, es decir, tal que

$$(\forall x \in \operatorname{dom} R)(\forall y, z \in \operatorname{ran} R)(xRy \wedge xRz \to y = z).$$

2. Una *relación uno a uno*, notada $1 \to 1$ (o, sinónimamente, $1 : 1$), es una relación restringida en su dominio e imagen a los subconjuntos unitarios, es decir,

$$1 \to 1 = (1 \to V) \cap (V \to 1).$$

3. Una *relación muchos a muchos*, notada $U \to V$ (o, sinónimamente, $M : N$), es una relación cualquiera.

Teorema 11.14 (Caracterización de una relación uno a uno)
R es $(1 \to 1)$ si, y sólo si, R^{-1} es $(1 \to 1)$.

Teorema 11.15 (Caracterización de una relación uno a muchos)
R es $(1 \to V)$ si, y sólo si, R^{-1} es $(V \to 1)$.

Actividad 11.2

Propongamos ejemplos de relaciones uno a uno, uno a muchos, muchos a uno y muchos a muchos.

§ 11.10 Correspondencia, función, aplicación y operación

Como es costumbre cuando se trabaja explícitamente con correspondencias, funciones y aplicaciones, designémoslas por $f, g, h, \ldots$, en vez de por $R, S, T, \ldots$; las operaciones, genéricamente por $*$.

Definición 11.20.— A una relación diádica cualquiera $f \subseteq X \times Y$ también la denominamos *correspondencia de X en Y* (o, sinónimamente, *correspondencia en X de valor en Y* —o *valorada en Y*—).

Definición 11.21.— A una relación funcional cualquiera $f \subseteq X \times Y$ también la denominamos *función parcial* de X en Y.

Cuando trabajamos con funciones, en vez de escribir $f \subseteq X \times Y$ y $\langle x, y\rangle \in f$ o xfy, escribimos $f : X \longrightarrow Y$ y $f(x) = y$, respectivamente. Así destacamos la posible dependencia de y —la *variable dependiente*— de x —la *variable independiente*—.

Definición 11.22.— De una relación funcional tal que $\operatorname{dom} f = X$ —esto es, todo el conjunto inicial— decimos que es una *función total* o *aplicación* de X en Y.

En algunos textos se diferencia entre función inyectiva, sobreyectiva o biyectiva y aplicación inyectiva, sobreyectiva o biyectiva, reservando las denominaciones de *inyección*, *epiyección* y *biyección* para las últimas.

Observación 11.10.0.— Si $f : X \longrightarrow Y$ es una aplicación, se satisface:

0. f es inyectiva si, y sólo si,

$$(\forall y \in \operatorname{ran} f)(\exists! x \in X)(f(x) = y),$$

esto es, precisamente si

$$(\forall x, y \in X)(f(x) = f(y) \rightarrow x = y),$$

lo que equivale por la contrarrecíproca del condicional a que

$$(\forall x, y \in X)(x \neq y \rightarrow f(x) \neq f(y));$$

1. f es sobreyectiva si, y sólo si,

$$(\forall y \in Y)(\exists x \in X)(f(x) = y);$$

2. *R* es *biyectiva* precisamente si es inyectiva y sobreyectiva, esto es, si, y sólo si,

$$(\forall y \in Y)(\exists! x \in X)(f(x) = y).$$

Definición 11.23.— Una *ley de composición interna* u *operación* en X es una aplicación $*$ de $X \times X$ en X.

§ 11.11 Familias de conjuntos y elementos

Definición 11.24.— Sean I y X dos conjuntos; una *familia de elementos* de X con *conjunto de índices* I es una relación funcional de I en X con dominio I, *i. e.*, una aplicación de I en X. Es habitual representar dicha relación funcional por $(x_i)_{i\in I}$.

Observación 11.11.0.— Usamos paréntesis y no llaves porque puede ocurrir que $x_i = x_j$ para $i \neq j$, esto es, los elementos pueden estar repetidos. En cualquier caso, notemos que una familia de elementos de X no es más que una *sucesión indizada*[8] de elementos de X.

Definición 11.25.— Dado un conjunto I, una *familia de conjuntos* con conjunto de índices I es una relación funcional con dominio I.

Definición 11.26.— Dado un conjunto X y un conjunto $I \neq \emptyset$, llamamos *familia de subconjuntos* de X con conjunto de índices I a toda relación funcional de I en 2^X con dominio I. Como para el caso de elementos, también se usan paréntesis, así es habitual que representemos esta relación funcional por $(X_i)_{i\in I}$ —notemos igualmente su vista como sucesión indizada—.

Las operaciones entre subconjuntos quedan igualmente extendidas. Dada una familia de subconjuntos de X, las siguientes son las definiciones de la *unión e intersección* de la familia:

$$\bigcap_{i\in I} X_i = \{x \in X : (\forall i \in I)(x \in X_i)\},$$
$$\bigcup_{i\in I} X_i = \{x \in X : (\exists i \in I)(x \in X_i)\}.$$

También definimos el *producto cartesiano* de los conjuntos de la familia,

$$\prod_{i\in I} X_i = \left\{ R \subseteq I \times \bigcup_{i\in I} X_i : \forall i \in I, \mathrm{im}_R\{i\} \in X_i \right\}.$$

Observación 11.11.1.— Como sabemos, $\forall i \in I, Pi$ es una abreviatura de $\forall i(i \in I \to Pi)$.

[8] *Cfr. supra* pág. lxxxiii de esta edición.

De esta definición se deriva la ya vista de producto cartesiano de un número finito de conjuntos. Por ejemplo, en el caso de dos conjuntos X e Y,

$$\begin{aligned} X \times Y &= \{R \subseteq \{0,1\} \times (X \cup Y) : \mathrm{im}_R\{0\} \in X \wedge \mathrm{im}_R\{1\} \in Y\} \\ &= \{R \subseteq \{0,1\} \times (X \cup Y) : \{x \in X \cup Y : \langle 0, x\rangle \in R\} \in X \wedge \{y \in X \cup Y : \langle 1, y\rangle \in R\} \in Y\} \\ &= \ldots = \{\langle x, y\rangle : x \in X \wedge y \in Y\}\,. \end{aligned}$$

Definición 11.27.— Dada una familia $(X_i)_{i\in I}$ de subconjuntos de X, indexada por I, decimos que una familia $(x_i)_{i\in I}$ de elementos de X es un *sistema de representantes* de $(X_i)_{i\in I}$ precisamente si $\forall i \in I, x_i \in X_i$ —también decimos que es un *multiconjunto de representantes* de X en su vista como multiconjunto $\{\{x_i\}\}_{i\in I}$—. En el caso de ser distintos los elementos x_i ($\forall i \in I$) decimos que $(x_i)_{i\in I}$ es un *sistema de representantes distintos* de la familia de conjuntos dada —también decimos que es un *conjunto de representantes* de X en su vista como conjunto $\{x_i\}_{i\in I}$; de hecho es habitual esta denominación y notación aunque se repitan los elementos—.

§ 11.12 Partición

Definición 11.28.— Denominamos *partición* de un conjunto X a toda familia de conjuntos $\{X_i\}_{i\in I}$ tal que I, II y III (a los subconjuntos X_i de la partición los llamamos *celdas*):

I. $(\forall i \in I)\,(X_i \neq \emptyset \wedge X_i \subseteq X)$; (todos los X_i son subconjuntos de X)

II. $(\forall i, j \in I)\,(i \neq j \rightarrow X_i \cap X_j = \emptyset)$; (los X_i son disjuntos dos a dos)

III. $\bigcup_{i\in I} X_i = X$ (la unión de todos los X_i es X).

Definición 11.29.— Si no se satisface la condición II, decimos que $\{X_i\}_{i\in I}$ es un *recubrimiento* (o, sinónimamente, *cobertura completa*) de X. En otras palabras, un recubrimiento de X es una familia $\mathcal{F}$ de subconjuntos no vacíos de X tal que la unión de todos los subconjuntos pertenecientes a $\mathcal{F}$ es X.

Observación 11.12.0.— Pudiésemos, pues, definir partición a partir de recubrimiento; una partición es un conjunto P de subconjuntos no vacíos de un conjunto no vacío X, que es recubrimiento de X y tal que cualesquiera dos subconjuntos distintos pertenecientes a P son disjuntos (los conjuntos de P son disjuntos dos a dos).

Teorema 11.16

Toda partición de X es un recubrimiento de X, pero no todo recubrimiento de X es una partición de X.

Definición 11.30.— Dadas dos particiones (resp., recubrimientos) P_0 y P_1 de un conjunto X, decimos que P_0 es una *partición más fina* (resp., *recubrimiento más fino*) que P_1 si cada conjunto de P_0 es un subconjunto de algún conjunto de P_1. Una partición más fina también se conoce como *refinamiento*.

Ejemplo 321

Sean $X = \{x, y, z\}$, $X_0 = \{x, y\}$, $X_1 = \{y, z\}$ y $X_2 = \{z\}$. Entonces, $P_0 = \{X_0, X_2\}$ es partición de X, mientras que $P_1 = \{X_0, X_1\}$ no es partición de X, aunque sí recubrimiento; de hecho, P_0 es un recubrimiento más fino que P_1—ya que $X_0 \subseteq X_0$ y $X_2 \subseteq X_1$ (por ser $X_2 \subset X_1$)—.

Ejemplo 322

Dados dos conjuntos X e Y, demostremos que $\{X \setminus Y, X \cap Y, Y \setminus X\}$ es una partición de $X \cup Y$ (se permite que los conjuntos de la partición puedan ser $\emptyset$).

ⓘ No es válida una demostración ni diagramática ni gráfica.

[Cubit 64], [EFE 28.6.2023:2], [EFO 27.5.2025:2], [EFE 18.6.2025:2].

Resolución.— Demostrar que una colección de conjuntos $\{S_0, S_1, \ldots, S_k\}$ es partición de un conjunto C es demostrar que los S_i son subconjuntos de C, que los S_i son disjuntos dos a dos y que la unión de los S_i es C. Suele ser de interés que ninguno de los S_i sea $\emptyset$, si bien aquí se permite. Estudiemos, pues, el caso que nos ocupa.

I. *$X \setminus Y$, $X \cap Y$ e $Y \setminus X$ son subconjuntos de $X \cup Y$.*

En efecto,

- $x \in X \setminus Y \to x \in X$ [definición de $\setminus$] $\to x \in X \cup Y$ [definición de $\cup$],
- $x \in X \cap Y \to x \in X$ [definición de $\cap$] $\to x \in X \cup Y$ [definición de $\cup$],
- $x \in Y \setminus X \to x \in Y$ [definición de $\setminus$] $\to x \in X \cup Y$ [definición de $\cup$].

II. *$X \setminus Y$, $X \cap Y$ e $Y \setminus X$ son disjuntos dos a dos.*

En efecto:

- $(X \setminus Y) \cap (X \cap Y) = (X \cap Y^{\complement}) \cap (X \cap Y)$ [definición de $\setminus$] $= (X \cap X) \cap (Y \cap Y^{\complement})$ [asociativa y conmutativa de $\cap$] $= X \cap (Y \cap Y^{\complement})$ [idempotencia de $\cap$] $= X \cap \emptyset$ [ley de complementación] $= \emptyset$ [ley de dominación].
- $(X \setminus Y) \cap (Y \setminus X) = (X \cap Y^{\complement}) \cap (Y \cap X^{\complement})$ [definición de $\setminus$] $= (X \cap X^{\complement}) \cap (Y \cap Y^{\complement})$ [asociativa y conmutativa de $\cap$] $= \emptyset \cap \emptyset$ [ley de complementación] $= \emptyset$ [ley de dominación].

- $(X \cap Y) \cap (Y \setminus X) = (X \cap Y) \cap (Y \cap X^{\complement})$ [definición de $\setminus$] $= (X \cap X^{\complement}) \cap (Y \cap Y)$ [asociativa y conmutativa de $\cap$] $= (X \cap X^{\complement}) \cap Y$ [idempotencia de $\cap$] $= \emptyset \cap Y$ [ley de complementación] $= \emptyset$ [ley de dominación].

III. $(X \setminus Y) \cup (X \cap Y) \cup (Y \setminus X) = X \cup Y$.

En efecto, demostrémoslo por doble inclusión. Sea $Z = (X \setminus Y) \cup (X \cap Y) \cup (Y \setminus X)$.

- Demostremos que $Z \subseteq X \cup Y$. En efecto,

  si $x \in Z$, entonces $x \in X \setminus Y$ o $x \in X \cap Y$ o $x \in Y \setminus X$ [def. de $\cup$],
  si $x \in X \setminus Y$, entonces $x \in X$ [def. de $\setminus$], de donde $x \in X \cup Y$ [def. de $\cup$],
  si $x \in X \cap Y$, entonces $x \in X$ [def. de $\cap$], de donde $x \in X \cup Y$ [def. de $\cup$],
  si $x \in Y \setminus X$, entonces $x \in Y$ [def. de $\setminus$], de donde $x \in X \cup Y$ [def. de $\cup$].

- Demostremos que $X \cup Y \subseteq Z$. En efecto,

  si $x \in X \cup Y$, entonces $x \in X$ o $x \in Y$,
  si $x \in X$, entonces $x \in Y$ o $x \notin Y$,
  si $x \in Y$, entonces $x \in X \cap Y$ [def. de $\cap$], de donde $x \in Z$ [def. de $\cup$],
  si $x \notin Y$, entonces $x \in X \setminus Y$ [def. de $\setminus$], de donde $x \in Z$ [def. de $\cup$],
  si $x \in Y$, entonces $x \in X$ o $x \notin X$,
  si $x \in X$, entonces $x \in X \cap Y$ [def. de $\cap$], de donde $x \in Z$ [def. de $\cup$],
  si $x \notin X$, entonces $x \in Y \setminus X$ [def. de $\setminus$], de donde $x \in Z$ [def. de $\cup$]. ■

Teorema 11.17
Sean X e Y dos conjuntos, $\{X_i\}_{i \in I}$ una partición de X y $\{R_i\}_{i \in I}$ una familia de relaciones funcionales de X_i en Y —$(\forall i \in I)\,(R_i \subseteq X \times Y)$— tales que $\forall i \in I$, $\operatorname{dom} R_i = X_i$. Entonces $R = \bigcup_{i \in I} R_i$ es la única relación funcional de X en Y con dominio X que satisface que $\forall i \in I$, $X_i \upharpoonright R = R_i$.

Observación 11.12.1.— De interés: maneras de partir un conjunto en base a objetivos concretos.

§ 11.13 Propiedades básicas de las relaciones diádicas

Además de las propiedades ya vistas de inyectividad, sobreyectividad y biyectividad[9] y funcionalidad[10], en este subcapítulo y en algunos siguientes estudiamos más propiedades de las relaciones diádicas.

[9] *Cfr. supra* definición 11.15 (pág. 607 de esta edición).
[10] *Cfr. supra* definición 11.16 (pág. 607 de esta edición).

Definición 11.31.— Sea R una relación diádica definida en X. La relación R satisface en X la propiedad de:

0. *reflexividad* (R) si, y sólo si, $\mathrm{id}_X \subseteq R$, en otras palabras, si, y sólo si, $(\forall x \in X)(xRx)$;
1. *irreflexividad* (I) —o *antirreflexividad*— si, y sólo si, $\mathrm{id}_X \subseteq R^{\complement}$, o sea, si, y sólo si, $\mathrm{id}_X \cap R = \emptyset$, en otras palabras, si, y sólo si, $(\forall x \in X)(x\neg Rx)$;
2. *simetría* (S) si, y sólo si, $R \subseteq R^{-1}$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(xRy \to yRx)$;
3. *tricotomía* (Tc) si, y sólo si, $(\forall x, y \in X)(xRy \veebar yRx \veebar x = y)$;
4. *asimetría* (A) si, y sólo si, $R^{-1} \subseteq R^{\complement}$, o sea, si, y sólo si, $R \subseteq (R^{-1})^{\complement}$, esto es, si, y sólo si, $(\forall x, y \in X)(xRy \to y\neg Rx)$;
5. *antisimetría* (An) si, y sólo si, $R \cap R^{-1} \subseteq \mathrm{id}_X$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(xRy \wedge yRx \to x = y)$, es decir, si, y sólo si, $(\forall x, y \in X)(x \neq y \wedge xRy \to y\neg Rx)$;
6. *no-simetría* (nS) si, y sólo si, $R^{-1} \neq R$, en otras palabras, si, y sólo si, $(\exists x, y \in X)(yRx \veebar xRy)$;
7. *transitividad* (T) si, y sólo si, $R \circ R \subseteq R$, en otras palabras, si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge yRz \to xRz)$;
8. *completitud fuerte* (Cf) —también llamada *dicotomía*, *conexión* o *comparabilidad*— si, y sólo si, $R^{\complement} \subseteq R^{-1}$, esto es, si, y sólo si, $X \subseteq R \cup R^{-1}$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(x\neg Ry \to yRx)$, lo que equivale a $(\forall x, y \in X)(xRy \vee yRx)$.

Teorema 11.18

Una relación R es transitiva si, y sólo si, $\forall n \in \mathbb{N}$, $R^n \subseteq R$.

Ejemplo 323

- *Reflexiva* es la relación de inclusión en el conjunto potencia de cualquier conjunto; también lo son las relaciones $\leq$ y $\geq$, en cualquier subconjunto de números reales.
- *Antirreflexiva* es la relación de perpendicularidad en el conjunto de las rectas del plano; también lo son las relaciones $<$ y $>$, en cualquier subconjunto de números reales.
- *Simétrica* es la relación de paralelismo en el conjunto de las rectas del plano; también lo es la relación $=$ en cualquier subconjunto de números reales.
- *Antisimétrica* es la relación de divisibilidad en cualquier subconjunto de números enteros; también lo es la relación de inclusión en el conjunto potencia de cualquier conjunto y las relaciones $\leq, \geq, <$ y $>$, en cualquier subconjunto de números reales.

- *Transitiva* es la relación de inclusión en el conjunto potencia de cualquier conjunto; también lo son las relaciones $\leq$, $\geq$, $<$ y $>$, en cualquier subconjunto de números reales y la de divisibilidad en cualquier subconjunto de números enteros; no lo es, por ejemplo, la relación de perpendicularidad en el conjunto de las rectas del plano.

- *Asimétrica* son las relaciones $<$ y $>$, en cualquier subconjunto de números reales; no lo es la relación de inclusión en el conjunto potencia de cualquier conjunto no vacío y no unitario.

- La relación «ser hermano de» es *antirreflexiva* (nadie es hermano de sí mismo), *simétrica* (si A es hermano de B, entonces B es hermano de A) y *transitiva* (si A es hermano de B, y B es hermano de C, entonces A es hermano de C). Esta relación es un ejemplo de *orden parcial estricto simétrico* —*cfr. infra* definición 11.52 (pág. 646 de esta edición)—.

- Un ejemplo de relación *transitiva* y *no tricótoma*: $R = X \times X$, con X un conjunto de más de un elemento.

Ejemplo 324

¿Es necesariamente transitiva la unión de dos relaciones transitivas?

[PEP 10.4.2019:2a].

Resolución.— No. Por ejemplo, sea el conjunto $C = \{0, 1, 2, 3\}$ y las relaciones diádicas definidas en C:

$$R = \{\langle 0, 1\rangle, \langle 1, 2\rangle, \langle 0, 2\rangle\},$$

$$S = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle\}.$$

Es trivial, por definición de transitividad, que ambas relaciones son transitivas en C; sin embargo, su unión,

$$R \cup S = \{\langle 0, 1\rangle\langle 1, 2\rangle, \langle 0, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle\},$$

es una relación diádica en C que no es transitiva en C, pues $\exists x, y, z \in C$, tales que x está relacionado con y e y con z pero x no lo está con z, por ejemplo, $x = 0$, $y = 1$ y $z = 3$, ya que $\langle 0, 1\rangle, \langle 1, 3\rangle \in R \cup S$, pero $\langle 0, 3\rangle \notin R \cup S$. ■

Observación 11.13.0.— Si una relación R es transitiva en un conjunto A, entonces es frecuente en ciertos ámbitos decir que z *depende transitivamente* de x a través de y si ocurre xRy e yRz. Si además es funcional se habla de *dependencia funcional transitiva*.

Ejemplo 325

En un conjunto, ¿cuántas y cuáles son las relaciones a la vez simétricas y antisimétricas?

Resolución.— Sea X un conjunto. Recordemos: R es simétrica si, y sólo si, $R \subseteq R^{-1}$, y es antisimétrica si, y sólo si, $R \cap R^{-1} \subseteq \mathrm{id}_X$. De ser simétrica, esto es, de $R \subseteq R^{-1}$, se sigue que $R \cap R^{-1} = R$, por lo que al ser antisimétrica, $R \subseteq \mathrm{id}_X$. En otras palabras, las únicas relaciones a la vez simétricas y antisimétricas en un conjunto X son las que sus elementos sean de la forma $\langle x, x \rangle$, con $x \in X$, esto es, las relaciones $\{\langle x, x \rangle : x \in S \wedge S \subseteq X \wedge S \neq \emptyset\}$, por lo que su número, al formarse a partir de los subconjuntos de x salvo el vacío es $2^{|X|} - 1$. Por ejemplo, si $X = \{0, 1\}$, existen tres ($2^2 - 1 = 3$): $\{\langle 0, 0 \rangle\}$, $\{\langle 1, 1 \rangle\}$ y $\{\langle 0, 0 \rangle, \langle 1, 1 \rangle\}$, y si $X = \{0, 1, 2\}$, existen siete ($2^3 - 1 = 7$): $\{\langle 0, 0 \rangle\}$, $\{\langle 1, 1 \rangle\}$, $\{\langle 2, 2 \rangle\}$, $\{\langle 0, 0 \rangle, \langle 1, 1 \rangle\}$, $\{\langle 0, 0 \rangle, \langle 2, 2 \rangle\}$, $\{\langle 1, 1 \rangle, \langle 2, 2 \rangle\}$ y $\{\langle 0, 0 \rangle, \langle 1, 1 \rangle, \langle 2, 2 \rangle\}$. ■

Ejemplo 326

Investiguemos las posibilidades entre ser o no ser irreflexiva y ser o no ser antisimétrica.

[EFEC 29.1.2025:4] (tipo test).

Resolución.— Sea $A = \{0, 1\}$, entonces:

- $R = \{\langle 0, 1 \rangle\}$ es una relación irreflexiva y antisimétrica en A;
- $R = \{\langle 0, 1 \rangle, \langle 1, 0 \rangle\}$ es una relación irreflexiva y no antisimétrica en A;
- $R = \{\langle 0, 0 \rangle\}$ es una relación no irreflexiva y antisimétrica en A;
- $R = \{\langle 0, 0 \rangle, \langle 0, 1 \rangle, \langle 1, 0 \rangle\}$ es una relación no irreflexiva y no antisimétrica en A.

Deducimos que pueden darse las cuatro posibilidades, es decir, que una relación en un conjunto puede ser:

- irreflexiva y antisimétrica;
- irreflexiva y no antisimétrica;
- no irreflexiva y antisimétrica;
- no irreflexiva y no antisimétrica. ■

Actividad 11.3

¿Ser R *tricótoma* equivale a $(\forall x, y \in X)(xRy \wedge x \neq y \rightarrow y \neg R x)$?

§ 11.14 Relaciones y operaciones de conjuntos

Las relaciones son conjuntos. Cuando operamos entre ellas con las operaciones de conjuntos, ¿qué ocurre? ¿Se conservan las propiedades? El siguiente teorema muestra lo que puede asegurarse para algunas operaciones y propiedades básicas, además de para la relación inversa.

Teorema 11.19 (Algunos resultados sobre propiedades y operaciones)
Sean dos relaciones diádicas P y Q. En este cuadro-resumen apreciamos la transmisión de las propiedades reflexiva, irreflexiva, simétrica, asimétrica, antisimétrica y transitiva, a las relaciones unión, intersección, complementaria, diferencia, diferencia simétrica e inversa.

P	Q	$P \cup Q$	$P \cap Q$	$P^{\complement}$	$P \setminus Q$	$P \triangle Q$	P^{-1}
R	R	R	R	I	I	I	R
I	I	I	I	R	R	R	I
S	S	S	S	S	S	S	S
A	A		A		A		A
An	An		An		An		An
T	T		T		T		T

El teorema anterior tiene como hipótesis la satisfacción de una propiedad por parte de dos relaciones y como tesis si dicha propiedad es satisfecha por la relación resultante de la operación. Pero, ¿y al revés?. Un breve ejemplo sobre la reflexiva es el siguiente.

Ejemplo 327

Sean R y S dos relaciones definidas en un conjunto X, ¿cuál de las siguientes afirmaciones es verdadera?

a. Si $R \cup S$ es reflexiva, R y S son reflexivas.
b. Si $R^{\complement} \cap S^{\complement}$ es reflexiva, R y S son reflexivas.
c. Si $R \circ R$ es reflexiva, R es reflexiva.
d. Si R^{-1} es reflexiva, R es reflexiva.

[TT], [EFE 3.7.2024:4] (tipo test).

Resolución.— La afirmación de la opción a) no es verdadera; sirva como contraejemplo éste: $X = \{0, 1\}$, $R = \{\langle 0, 0\rangle, \langle 0, 1\rangle\}$ y $S = \{\langle 0, 1\rangle, \langle 1, 1\rangle\}$; entonces, $R \cup S = \{\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 1, 1\rangle\}$ es reflexiva en X, pero ni R ni S son reflexivas en X, pues $\langle 1, 1\rangle \notin R$ y $\langle 0, 0\rangle \notin S$.

La afirmación de la opción b) no es verdadera, ya que si $\langle x, x\rangle \in R^{\complement} \cap S^{\complement}$, entonces $\langle x, x\rangle \notin R$ y $\langle x, x\rangle \notin S$, por lo que ni R ni S pueden ser reflexivas.

La afirmación de la opción c) no es verdadera, pues $\langle x, x\rangle \in R \circ R$ significa que existe $y \in X$ tal que $\langle x, y\rangle$ e $\langle y, x\rangle$, no que $\langle x, x\rangle \in R$ (si fuese transitiva, sí).

La afirmación de la opción d) es verdadera porque si $\langle x, x\rangle \in R^{-1}$, entonces $\langle x, x\rangle \in R$ —por definición de R^{-1}, a saber, $R^{-1} = \{\langle y, x\rangle : \langle x, y\rangle \in R\}$—.

Solución.— Opción d. ■

Ejemplo 328

Sean $^{-1}$, $\cup$, $\cap$ y $\circ$ las operaciones inversa, unión, intersección y composición de relaciones, respectivamente. Sean R y S dos relaciones definidas en un conjunto X, ¿cuál de las siguientes afirmaciones es verdadera?

a. Si R y S son transitivas, $R \cup S$ es transitiva.
b. Si R es transitiva, $R^{\complement}$ es transitiva.
c. Si R y S son transitivas, $R \circ S$ es transitiva.
d. Si R es transitiva, R^{-1} es transitiva.

[TT], [EFE 29.1.2025:4] (tipo test).

Resolución.— La afirmación de la opción a) no es verdadera; sirva como contraejemplo éste: $X = \{x, y, z, w\}$, $R = \{\langle x, y\rangle, \langle y, z\rangle, \langle x, z\rangle\}$ y $S = \{\langle y, z\rangle, \langle z, w\rangle, \langle y, w\rangle\}$, ambas transitivas; sin embargo, $R \cup S$ no es transitiva, pues $\langle x, y\rangle \in R \cup S$ y $\langle y, w\rangle \in R \cup S$, pero $\langle x, w\rangle \notin R \cup S$.

La afirmación de la opción b) no es verdadera; sirva como contraejemplo éste: $X = \mathbb{N}$, $R = \{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} : x \leq y\}$; R es transitiva en $\mathbb{N}$ por serlo $\leq$; sin embargo, $R^{\complement} = \{\langle x, y\rangle \in \mathbb{N} \times \mathbb{N} : x > y\}$ no es transitiva, pues si $x > y$ e $y > z$, no necesariamente se satisface que $x > z$ —por ejemplo, si $x = 2$, $y = 1$ y $z = 0$, entonces $2 > 1$ y $1 > 0$, pero también $2 > 0$—.

La afirmación de la opción c) no es verdadera; sirva como contraejemplo éste: $X = \{0, 1, 2\}$, $R = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 1, 2\rangle\}$, $S = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 0, 1\rangle\}$, ambas transitivas; sin embargo, $R \circ S = \{\langle x, z\rangle \in X \times X : (\exists y \in X)(xSy \wedge yRz)\} = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 0, 1\rangle, \langle 1, 2\rangle\}$ no es transitiva, pues $\langle 0, 1\rangle \in R \circ S$ y $\langle 1, 2\rangle \in R \circ S$, pero $\langle 0, 2\rangle \notin R \circ S$.

La afirmación de la opción d) es verdadera porque si $\langle x, y\rangle \in R^{-1}$ e $\langle y, z\rangle \in R^{-1}$, entonces $\langle y, x\rangle \in R$ y $\langle z, y\rangle \in R$ —por definición de R^{-1} (a saber, $R^{-1} = \{\langle y, x\rangle : \langle x, y\rangle \in R\}$)—, de donde, por ser R transitiva en X, $\langle z, x\rangle \in R$, de donde, $\langle x, z\rangle \in R^{-1}$ —por definición de R^{-1}—, en otras, palabras, R^{-1} es transitiva en X.

Solución.— Opción d. ■

§ 11.15 Descomposición por simetría de una relación diádica

Es posible descomponer toda relación diádica R en X en dos componentes, su componente asimétrica y su componente simétrica.

Definición 11.32.— La *componente asimétrica* —que notamos R_{A}— de una relación R en un conjunto X queda definida por

$$(\forall x, y \in X)(xR_{\mathrm{A}}y \leftrightarrow xRy \wedge y\neg Rx).$$

Definición 11.33.— La *componente simétrica* —que notamos R_{S}— de una relación R en un conjunto X queda definida por

$$(\forall x, y \in X)(xR_{\mathrm{S}}y \leftrightarrow xRy \wedge yRx).$$

Igualmente, dada una relación diádica R en X es posible descomponer su relación complementaria en dos componentes: la relación de incomparabilidad por R en X y la inversa de la componente asimétrica de R en X.

Definición 11.34.— La *relación de incomparabilidad* por R —que notamos R_{I}— en X es la relación diádica definida por

$$(\forall x, y \in X)(xR_{\mathrm{I}}y \leftrightarrow x\neg Ry \wedge y\neg Rx).$$

Teorema 11.20

Se satisface:

0. $R = R_{\mathrm{A}} \cup R_{\mathrm{S}}$;
1. $R^{\complement} = R_{\mathrm{I}} \cup R_{\mathrm{A}}^{-1}$.

§ 11.16 Detección matricial de propiedades de endorrelaciones

La observación de la matriz lógica nos permite detectar algunas propiedades. Vamos a partir de las definiciones para encontrarlas:

- R es *reflexiva* en X si, y sólo si, $\mathrm{id}_X \subseteq R$, es decir, si, y sólo si, todos los elementos de la diagonal principal de su matriz lógica M_R son unos, esto es, precisamente si $m_{ii} = 1$, para todo i;
- R es *irreflexiva* en X si, y sólo si, $\mathrm{id}_X \subseteq R^{\complement}$, esto es, si, y sólo si, $\mathrm{id}_X \cap R = \emptyset$, en otras palabras, si, y sólo si, $(\forall x \in X)(x\neg Rx)$, es decir, todos los elementos de la diagonal principal de su matriz lógica M_R son ceros, en definitiva, si, y sólo si, $m_{ii} = 0$, para todo i;

- R es *simétrica* si, y sólo si, $R \subseteq R^{-1}$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(xRy \to yRx)$, es decir, si, y sólo si, su matriz lógica M_R es simétrica, esto es, si, y sólo si, $m_{ij} = m_{ji}$, para todo i, j;

- R es *antisimétrica* si, y sólo si, $R \cap R^{-1} \subseteq \mathrm{id}_X$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(xRy \wedge yRx \to x = y)$, es decir, si, y sólo si, $(\forall x, y \in X)(x \neq y \wedge xRy \to y \neg Rx)$, en definitiva, si, y sólo si, en su matriz lógica M_R ocurre que para todo i, j, con $i \neq j$, $m_{ij} = 0$ o $m_{ji} = 0$—o ambos (o inclusivo)—, en otras palabras, si, y sólo si, el par ordenado (m_{ij}, m_{ji}), con $i \neq j$, puede ser $(0, 0)$, $(0, 1)$ o $(1, 0)$;

- R es *asimétrica* si, y sólo si, es irreflexiva y antisimétrica, es decir, si, y sólo si, $m_{ii} = 0$, para todo i, y para todo i, j, con $i \neq j$, $m_{ij} = 0$ o $m_{ji} = 0$;

- R es *transitiva* si, y sólo si, $R \circ R \subseteq R$, en otras palabras, si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge yRz \to xRz)$, es decir, si, y sólo si, para todos los elementos no nulos del cuadrado M_R^2 de su matriz lógica M_R, el elemento correspondiente de esta última es un uno, en definitiva, si, y sólo si, $\forall i, j, m_{ij}^2 \neq 0 \to m_{ij} \neq 0$;

- R es *conexa (fuertemente completa)* si, y sólo si, $R^{\complement} \subseteq R^{-1}$, esto es, si, y sólo si, $M^T - M^{\complement} \geq 0$, donde M^T es la traspuesta de M y $M^{\complement}$ se construye a partir de M intercambiando los ceros con los unos.

Observación 11.16.0.— Con respecto a la detección matricial de la transitividad en una relación, consultemos la página web correspondiente a esta pregunta en Mathematics Stack Exchange[11].

El apartado (3) de la respuesta posicionada en primer lugar proporciona un buen ejemplo razonado de cómo se usa la matriz lógica de una relación y su cuadrado para detectar la transitividad de una relación. Estudiémoslo, nos vendrá bien.

Por cierto, Stack Exchange es una metacomunidad con más de 180 comunidades especializadas[12]. Explorémoslas, seguro que más de una es de nuestro interés. Por ejemplo, Stack Overflow es una de las comunidades de la RUD (Red Universal Digital) que reúne a un mayor número de personas dedicadas a la programación[13]. Algo similar, si bien en Matemáticas, sucede con Mathematics[14].

§ 11.17 Detección de propiedades de relaciones en sus digrafos

La observación del digrafo nos permite detectar algunas propiedades.

[11] *Vid.* https://math.stackexchange.com/questions/228898/how-to-check-whether-a-relation-is-transitive-from-the-matrix-representation.
[12] *Vid.* https://stackexchange.com/sites. De hecho, si deseásemos crear una nueva comunidad en Stack Exchange, pudiésemos proponerlo en su Área 51: https://area51.stackexchange.com/.
[13] *Vid.* https://stackoverflow.com/questions.
[14] *Vid.* https://math.stackexchange.com/.

- R es *reflexiva* si, y sólo si, todos los vértices del digrafo G_R tienen un bucle.
- R es *irreflexiva* si, y sólo si, ningún vértice de su digrafo G_R tiene un bucle.
- R es *simétrica* si, y sólo si, sucede en su digrafo G_R que $\langle x, y\rangle$ es un arco si, y sólo si, $\langle y, x\rangle$ es un arco.
- R es *antisimétrica* si, y sólo si, sucede en su digrafo G_R que para cualesquiera $x \neq y$, si $\langle x, y\rangle$ es un arco, entonces $\langle y, x\rangle$ no es un arco.
- R es *transitiva* si, y sólo si, sucede en su digrafo G_R que para cualesquiera x, y, z, si $\langle x, y\rangle$ e $\langle y, z\rangle$ son arcos, entonces $\langle x, z\rangle$ es un arco.

§ 11.18 Más propiedades de las relaciones diádicas

Definición 11.35.— Decimos que una relación diádica $R \subseteq X \times X$ satisface en X la propiedad de ser:

0. *negativamente asimétrica* si, y sólo si, $R^{\complement} \subseteq R^{-1}$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(x \neg R y \rightarrow y R x)$;
1. *asimetría fuerte* (Af) si, y sólo si, $R \subseteq (R^{-1})^{\complement}$ y $R^{\complement} \subseteq R^{-1}$, en otras palabras, si, y sólo si, $(\forall x, y \in X)((xRy \rightarrow y\neg Rx) \wedge (x\neg Ry \rightarrow yRx))$, lo que equivale a $(\forall x, y \in X)(xRy \veebar yRx)$;
2. *negativamente transitiva* si, y sólo si, $R^{\complement} \circ R^{\complement} \subseteq R^{\complement}$, en otras palabras, si, y sólo si, $(\forall x, y, z \in X)(x\neg Ry \wedge y\neg Rz \rightarrow x\neg Rz)$;
3. *serial* (Se) si, y sólo si, $(\forall x \in X)(\exists y \in X)(xRy)$;
4. *euclidea* (E) si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge xRz \rightarrow yRz)$;
5. *completa* (C) —también llamada *semiconexa*— si, y sólo si, $R^{\complement} \subseteq R^{-1} \cup \mathrm{id}_X$, esto es, si, y sólo si, $(\mathrm{id}_X)^{\complement} \subseteq R \cup R^{-1}$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(x \neq y \rightarrow xRy \vee yRx)$, es decir, si, y sólo si, $(\forall x, y \in X)(x \neq y \wedge x\neg Ry \rightarrow yRx)$;
6. *circular* (Ci) si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge yRz \rightarrow zRx)$;
7. *acíclica* (Aci) si, y sólo si, $(\forall n > 0)(\forall x_0, x_1, \ldots, x_n \in X)(\neg(x_0 R_A x_1 \wedge x_1 R_A x_2 \wedge \ldots \wedge x_{n-1} R_A x_n \wedge x_n R_A x_0))$.

Con el siguiente teorema iniciamos una colección de interrelaciones —*cfr. v. gr.* Jansana [160] (pág. 58); Ríos Insúa, Bielza Lozoya y Mateos Caballero [161] (pág. 32); Mosterín [162] (pág. 199)— entre algunas de las propiedades listadas en las definiciones de este capítulo.

Teorema 11.21 (Algunas relaciones entre las propiedades, I)
Sea R una relación diádica definida en un conjunto no vacío X, entonces:

a. si R es reflexiva, entonces R es serial;
b. si R es irreflexiva, transitiva y fuertemente completa —esto es, si R es un orden total estricto—, entonces R es negativamente transitiva;
c. si R es reflexiva y euclidea, entonces R es simétrica y transitiva (R es de equivalencia parcial) —y como es reflexiva, resulta que R es una relación de equivalencia—;
d. si R es simétrica y transitiva —esto es, si R es de equivalencia parcial—, entonces R es euclidea;
e. si R es reflexiva, entonces ser R euclidea equivale a ser R simétrica y transitiva (ser R de equivalencia parcial);
f. si R es simétrica y euclidea, entonces R es transitiva;
g. si R es simétrica, entonces ser R euclidea equivale a ser R transitiva;
h. si R es simétrica, transitiva y serial —esto es, si R es serial y de equivalencia parcial—, entonces R es reflexiva;
i. si R es tricótoma, entonces R es asimétrica;
j. R es asimétrica si, y sólo si, R es irreflexiva y antisimétrica;
k. R es asimétrica y fuertemente completa si, y sólo si, R es fuertemente asimétrica;
l. si R es asimétrica y negativamente transitiva —esto es, si R es una relación de preferencia estricta (un orden débil estricto)—, entonces R es transitiva;
m. si R es transitiva, entonces ser R asimétrica equivale a ser R irreflexiva;
n. R es fuertemente completa, si, y sólo si, R es reflexiva y completa;
ñ. R es fuertemente completa si, y sólo si, $R^{\complement}$ es asimétrica;
o. R es completa si, y sólo si, $R^{\complement}$ es antisimétrica;
p. si R es simétrica y transitiva —esto es, si R es de equivalencia parcial—, entonces R es circular;
q. si R es reflexiva y circular, entonces R simétrica y transitiva (R es de equivalencia parcial);
r. R es reflexiva, simétrica y transitiva (R es de equivalencia) si, y sólo si, R es reflexiva y circular.

§ 11.19 Otras propiedades

Definición 11.36.— Dado un conjunto X, decimos que una relación diádica R satisface en X la propiedad de:

0. *idempotencia* (Id) si, y sólo si, $R \circ R = R$, en otras palabras, si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge yRz \leftrightarrow xRz)$;

1. *intransitividad* (iT) si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge yRz \to x\neg Rz)$;

2. *dirección* (Di) si, y sólo si, $X \subseteq R^{-1} \circ R$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(\exists z \in X)(xRz \wedge yRz)$;
3. *contradirección* (Cdi) si, y sólo si, $X \subseteq R \circ R^{-1}$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(\exists z \in X)(zRx \wedge zRy)$;
4. *proyección*[15](F) si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge xRz \rightarrow y = z)$;
5. *proyección* X^X (Fc) si, y sólo si, $(\forall x \in X)(\exists! y \in X)(xRy)$;
6. *asignación* (As) si, y sólo si, $(\forall x, y, z \in X)(yRx \wedge zRx \rightarrow y = z)$;
7. *densidad débil* (D) si, y sólo si, $R \subseteq R \circ R$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(xRy \rightarrow (\exists z \in X)(xRz \wedge zRy))$;
8. ser *débilmente dirigida* (Dd) si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge xRz \rightarrow (\exists t \in X)(yRt \wedge zRt))$;
9. *completitud débil* (Cd) si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge xRz \rightarrow yRz \vee zRy \vee y = z)$;
10. Ferrers (Fe) si, y sólo si, $(\forall x, y, z, t \in X)(xRy \wedge zRt \rightarrow xRt \vee zRy)$;
11. *semi-transitividad* (sT) si, y sólo si, $(\forall x, y, z \in X)(xRy \wedge yRz \rightarrow (\exists t \in X)(xRt \vee tRz))$;
12. *cuasitransitividad* (cT) si, y sólo si, R_A —su componente asimétrica— es transitiva;
13. *trivialidad* (Tr) si, y sólo si, $X \subseteq R$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(xRy)$;
14. *vacuidad* (V) si, y sólo si, $X \subseteq R^{\complement}$, en otras palabras, si, y sólo si, $(\forall x, y \in X)(x \neg R y)$.

Observación 11.19.0.— Jesús Mosterín [162] (cap. 10) discute la relación entre las propiedades de *proyección* y *asignación*, las posibles definiciones de *composición de relaciones diádicas*, las consecuentes *definiciones de función* y la relación de todo ello con nuestro *lenguaje natural*. Si $R \circ S$ se define como $(\forall a, b \in C)(a(R \circ S)b \leftrightarrow (\exists c \in C)(aSc \wedge cRb)$ —en desacuerdo con nuestro lenguaje natural (sea por ejemplo R «ser hermano de» y S «ser padre de» , queriendo $R \circ S$ expresar la relación «ser tío de» , que en nuestro lenguaje natural significa «ser hermano del padre de»)—, entonces, para funciones, $(f \circ g)(x) = f(g(x))$ —de acuerdo con nuestra intuición matemática—; sin embargo, si $R \circ S$ se define como $(\forall a, b \in C)(a(R \circ S)b \leftrightarrow (\exists c \in C)(aRc \wedge cSb)$ —de acuerdo con nuestro lenguaje natural—, entonces, para funciones, $(f \circ g)(x) = g(f(x))$ —en contra de nuestra intuición matemática. Esperando que nos haya interesado esta pequeña reseña, aprenderemos más estudiando el mencionado capítulo 10 de [162].

Teorema 11.22 (Algunas relaciones entre las propiedades, II)
Sea R es una relación diádica definida en un conjunto no vacío X, entonces:

s. si R es reflexiva, antisimétrica, transitiva y fuertemente completa[16], entonces R satisface las propiedades de dirección y contradirección;
t. si R es intransitiva, entonces R es irreflexiva;
u. si R es trivial, entonces R es fuertemente completa.

§ 11.20 Estructuras relacionales diádicas: géneros destacados

En la familia de relaciones diádicas destacamos dos géneros, las clasificaciones y las ordenaciones. En el primero, destacamos dos especies, las equivalencias y las tolerancias (también llamadas compatibilidades); en el segundo, los órdenes y las preferencias. Esto es,

- clasificaciones:
  - equivalencias (parciales y totales), y
  - tolerancias (compatibilidades);
- ordenaciones:
  - órdenes, y
  - preferencias.

De ellas hablamos en los artículos siguientes.

§ 11.21 Relación de equivalencia parcial

§ 11.21.0 Simetría

La simetría parece la base de cualquier relación precisa de clasificación: dadas dos entidades E y F, si E se clasifica en la misma clase que F, parece lógico que F se clasifique en la misma clase que E.[17]

[16] Anticipamos que estas relaciones se conocen como *órdenes totales* —*cfr. infra* definición 11.26.3 (pág. 648 de esta edición)—.

[17] «*Exact symmetry only exists in the mathematician's mind. It is never achieved in the real world, neither in nature nor in man-made objects* [La simetría exacta solo existe en la mente del matemático. Nunca se alcanza en el mundo real, ni en la naturaleza ni en los objetos hechos por el hombre]» (Alexei Vasilievich Shubnikov y Vladimir Alexandrovich Koptsik, *Symmetry in Science and Art*, Nueva York: Plenum Press, 1974 [*cfr. v. gr.* https://en.wikipedia.org/wiki/Symmetry_in_Science_and_Art]).

Definición 11.37.— Decimos que $R \subseteq X \times X$ es una *relación de adyacencia* en X precisamente si R es simétrica e irreflexiva en X.

Ejemplo 329

Dado un conjunto X, las siguientes dos relaciones son de adyacencia en 2^X, esto es, si cumplen las condiciones exigidas los subconjuntos se clasifican en la misma clase. En su representación como grafos no dirigidos (por ser simétricas), éstos no tienen bucles. Definimos estas relaciones, $\forall U, V \subseteq X$, por:

0. $UR_\triangle V$ si, y sólo si, $|U \setminus V| = |V \setminus U| = 1$;

1. $UR_H V$ si, y sólo si, $|U \setminus V| - |V \setminus U| = \pm 1$.

§ 11.21.1 Simetría más transitividad: equivalencia parcial

La transitividad, añadida, implica que las clases definidas por la simetría sean disjuntas.

Definición 11.38.— Decimos que $R \subseteq X \times X$ es una *relación de equivalencia parcial* (abreviadamente, EQ o PER) en X precisamente si R es simétrica y transitiva en X. También decimos entonces que X es un conjunto parcialmente clasificado por R o que $(X; R)$ es un *conjunto parcialmente clasificado*.

Ejemplo 330

Propongamos un ejemplo de relación de equivalencia parcial entre personas.

Resolución.— La relación «ser hermana de» es una relación de equivalencia parcial entre personas, pues es simétrica (si la persona A es hermana de la persona B, entonces B es hermana de A) y es transitiva (si A es hermana de B y B es hermana de C, entonces A es hermana de C). ■

Ejemplo 331

¿Cuál de las siguientes relaciones entre personas es de equivalencia parcial?

a. xRy si, y sólo si, tienen la misma afición.
b. xRy si, y sólo si, se conocen.
c. xRy si, y sólo si, van al mismo gimnasio.
d. xRy si, y sólo si, tienen opiniones opuestas y están de acuerdo en todo.

[TT], [EFE 29.1.2025:5] (tipo test).

Resolución.— Analicemos cada relación:

a. No tiene por qué ser transitiva: pensemos en x con la sola afición A, y con las aficiones A y B, y z con la única afición B.

b. No tiene por qué ser transitiva: pudiese suceder que x e y se conociesen y que y y z también, pero x y z no se conociesen.

c. No tiene por qué ser transitiva: pudiese suceder que x asiste sólo al gimnasio A, y asista a los gimnasios A y B, y z asista únicamente al gimnasio B.

d. Se trata de la relación vacía, que es de equivalencia parcial (simétrica y transitiva) por vacuidad.

Solución.— Opción d. ■

Actividad 11.4

¿Cuál de las siguientes relaciones entre personas es de equivalencia parcial?

a. xRy si, y sólo si, son amigas.
b. xRy si, y sólo si, son vecinas.
c. xRy si, y sólo si, están en el mismo club de lectura.
d. xRy si, y sólo si, están físicamente juntas, ambas en Cáceres y ambas en Badajoz, al mismo tiempo.

[TT], [EFEC 29.1.2025:5] (tipo test).

Observación 11.21.0.— La relación «ser hermana de» no es reflexiva en el conjunto de las personas, pues ninguna persona es hermana de sí misma. Por otra parte, la relación vacía sólo es reflexiva en el conjunto vacío; no lo es en un conjunto no vacío, pues existe al menos un elemento no relacionado consigo mismo. Completar una relación de equivalencia parcial con la reflexiva y obtener así un conjunto clasificado completamente es el tema del artículo siguiente.

§ 11.22 Relación de equivalencia

Las relaciones reflexivas de *clasificación* (*cfr.* Fig. 11.6), esto es, las relaciones simétricas, transitivas y reflexivas, son conocidas como *equivalencias*.

Observación 11.22.0.— De nuevo, pensemos en la no importancia de la reflexividad, al menos sin completitud o serialidad. Observemos, por ejemplo, el siguiente razonamiento erróneo: «Sea R una relación simétrica y transitiva en X. Sean $x, y \in X$ tales que xRy. De la simetría de R deducimos que yRx. Luego, $xRy \wedge yRx$. De la transitividad de R resulta que xRx. Por tanto, la relación R es reflexiva en X.» —*cfr.* Alonso Jiménez, Borrego Díaz, Pérez Jiménez y Ruiz Reina [142] (pág. 36)—.

Definición 11.39.— Decimos que $R \subseteq X \times X$ es una *relación de equivalencia* (abreviadamente, EQV) en X precisamente si es una relación de equivalencia parcial reflexiva, esto es, si, y sólo si, es reflexiva, simétrica y transitiva en X. De un par de elementos de X relacionados por una tal R decimos que son *equivalentes*, y dependiendo de las circunstancias también decimos que son *semejantes*, *congruentes* o *isomorfos*. También decimos entonces que X es un conjunto clasificado por R o que $(X; R)$ es un *conjunto clasificado*.

Designaciones frecuentes por las que se expresa una relación de equivalencia y por tanto, la equivalencia de dos elementos, son $x \sim y$, $x \approx y$, $x \cong y$, $x \equiv y$, $x \leftrightarrow y$, $x \Leftrightarrow y$.

Ejemplo 332

¿Cuál de las siguientes relaciones entre personas es de equivalencia?

a. xRy si, y sólo si, hablan el mismo idioma.
b. xRy si, y sólo si, se conocen.
c. xRy si, y sólo si, y es, bien la misma persona que x, bien el padre de x.
d. xRy si, y sólo si, son paisanas.

[TT], [EFE 3.7.2024:5] (tipo test).

Resolución.— Ni hablar el mismo idioma ni conocerse son relaciones transitivas (por ejemplo: X sólo habla español, Y habla español y portugués, Z sólo habla portugués; X e Y se conocen, Y y Z se conocen, pero X y Z no se conocen), por lo que quedan descartadas las opciones a) y b). En cuanto a la relación dada en la opción c), es reflexiva por definición, no es simétrica (no soy el padre de mi padre) y no es transitiva (el padre de mi padre no es mi padre). La relación dada en d) sí es de equivalencia: ser paisanas, esto es, ser natural del mismo país, provincia o lugar, sí que satisface la reflexividad, la simetría y la transitividad.

Solución.— Opción d. ∎

Ejemplo 333

Sea C un conjunto y R una relación diádica definida en C. Consideremos las propiedades ser R sobreyectiva —$(\forall y \in C)(\exists x \in C)(xRy)$— y ser euclidea —$(\forall a, b, c \in C)(aRb \wedge aRc \rightarrow bRc)$—. Demostremos que:

0. si R es de equivalencia en C, entonces R es sobreyectiva y euclidea en C;
1. recíprocamente, si R es sobreyectiva y euclidea en C, es de equivalencia en C.

[PEP 10.4.2019:2b].

Resolución.— En efecto:

0. demostremos que si R es reflexiva, simétrica y transitiva en C, entonces R es sobreyectiva y euclidea en C:

   - por ser R reflexiva, se tiene que $\forall y \in C, yRy$ y por tanto, se satisface que R es sobreyectiva en C (x es el propio y);
   - por otro lado, por ser R simétrica, de $(xRy \wedge xRz)$ se sigue $(yRx \wedge xRz)$ y de éste, por ser transitiva, (yRz), por lo que R es euclidea en C;

1. demostremos que si R es sobreyectiva y euclidea en C, entonces R es reflexiva, simétrica y transitiva en C:

   - por ser R sobreyectiva en C, tenemos que $\forall y \in C, \exists x \in C, xRy$, entonces, ser euclidea en C, de tener $xRy \wedge xRy$, se sigue que yRy y por tanto, que R es reflexiva en C;
   - supongamos que xRy, como es reflexiva, se tiene xRx, entonces por ser euclidea, yRx y por tanto, R es simétrica en C;
   - si $xRy \wedge yRz$, entonces, por ser simétrica, se tiene que $yRx \wedge yRz$, y de aquí, por ser euclidea, se tiene que xRz y por tanto, que R es transitiva en C. ■

Teorema 11.23
La relación de equivalencia más pequeña (abreviadamente, SER), en el sentido de la inclusión, en un conjunto X, es id_X.

Teorema 11.24
La relación de equivalencia más grande (abreviadamente, GER), en el sentido de la inclusión, en un conjunto X es el producto cartesiano $X \times X$.

§ 11.22.0 Clase de equivalencia

Definición 11.40.— Sea $(X; R)$ un conjunto clasificado. Llamamos *clase de equivalencia* (o, sinónimamente, *conjunto de elementos equivalentes*) de un elemento $x \in X$ a la imagen de $\{x\}$ por R,[18], esto es,

$$[x]_R = \{y \in X : \langle x, y\rangle \in R\}$$

es decir, al conjunto de todos los elementos de X relacionados con x —siendo también notaciones habituales $\mathrm{im}_R(x)$, $R(x)$ y $\bar{x}^R$—.

[18] *Cfr. supra* definición 11.8 (pág. 594 de esta edición).

Teorema 11.25
Si $(X; R)$ es un conjunto clasificado, entonces toda clase de equivalencia generada por R en X es no vacía, lo cual, expresado en lenguaje lógico-matemático es:

si $(X; R)$ es un conjunto clasificado, entonces $(\forall x \in X)([x]_R \neq \emptyset)$.

Demostración.— Dado $x \in X$, $[x]_R = \{y \in X : \langle x, y\rangle \in R\}$; como R es una equivalencia, R es reflexiva, es decir, $\langle x, x\rangle \in R$, de donde por definición de $[x]_R$, se tiene que $x \in [x]_R$ y por tanto, $[x]_R \neq \emptyset$. ∎

Una vez demostrado que no son vacías, en cada clase de equivalencia destacamos un elemento $x_{[x]_R}$ al que denominamos *representante* de la clase —un *arquetipo*, un *ejemplar*—. Este elemento sirve como identificador de la clase.

Ejemplo 334

En el conjunto $\mathbb{Z}$ de los números enteros, se define la relación diádica R: $\forall x, y \in \mathbb{Z}$, $xRy \leftrightarrow x^2 - y^2 = x - y$.

0. Demostremos que R es una relación de equivalencia en $\mathbb{Z}$.
1. Utilicemos la definición de clase de equivalencia para encontrar todos los números enteros pertenecientes a la clase de equivalencia de $a \in \mathbb{Z}$.

[Cubit 73], [EFE 29.6.2018:2], [EFE 19.1.2023:3], [EFO 24.5.2023:3], [EFO 27.5.2025:3], [EFE 18.6.2025:3].

Resolución.— Recordemos que decimos que una relación es de equivalencia en un conjunto precisamente si es reflexiva, simétrica y transitiva en dicho conjunto.

0.
   I. $\forall x \in \mathbb{Z}, x^2 - x^2 = x - x$, ya que ambos son iguales a cero, por lo que $\forall x \in \mathbb{Z}, xRx$, esto es, R es reflexiva en $\mathbb{Z}$;

   II. $\forall x, y \in \mathbb{Z}, x^2 - y^2 = x - y \leftrightarrow y^2 - x^2 = y - x$ [multiplicando ambos miembros de la igualdad por (-1)], por lo que $(\forall x, y \in \mathbb{Z})\ (xRy \rightarrow yRx)$, esto es, R es simétrica en $\mathbb{Z}$;

   III. $(\forall x, y, z \in \mathbb{Z})\ (x^2 - y^2 = x - y \wedge y^2 - z^2 = y - z \rightarrow x^2 - z^2 = x - z)$ [sumando miembro a miembro], por lo que $(\forall x, y, z \in \mathbb{Z})\ (xRy \wedge yRz \rightarrow xRz)$, esto es, R es transitiva en $\mathbb{Z}$.

   Luego R es una relación diádica de equivalencia en $\mathbb{Z}$.

1. $\forall a \in \mathbb{Z}$,

$$\begin{aligned}[a] &= \{x \in \mathbb{Z} : aRx\}\\ &= \{x \in \mathbb{Z} : a^2 - x^2 = a - x\}\\ &= \{x \in \mathbb{Z} : x^2 - x - a^2 + a = 0\}\\ &= \{a, 1 - a\},\end{aligned}$$

ya que de ser $x = (1 \pm \sqrt{1 + 4a^2 - 4a})/2 = (1 \pm \sqrt{(2a - 1)^2})/2 = (1 \pm (2a - 1))/2$, se siguen dos soluciones enteras, $x_0 = 2a/2 = a$ y $x_1 = (2 - 2a)/2 = 1 - a$, simples y distintas[19].

Solución.— Para todo número entero a, sólo dos números enteros pertenecen a la clase de equivalencia de a según la relación R, a saber, a y $1 - a$. ∎

Observación 11.22.1.— Al hacer el apartado 1 hemos demostrado que $(\forall x, y \in \mathbb{Z}), (xRy \leftrightarrow x = y \veebar x = 1 - y)$.

Observación 11.22.2.— Es posible que hubiésemos simplificado la definición de la relación, directamente, al comienzo (de paso, veamos otra vía, sin necesidad de resolver la ecuación de segundo grado), $(\forall x, y \in \mathbb{Z})$:

$$\begin{aligned} xRy &\leftrightarrow x^2 - y^2 = x - y \\ &\leftrightarrow (x - y)(x + y) = x - y \\ &\leftrightarrow x = y \veebar x + y = 1. \end{aligned}$$

Teorema 11.26
Si $(X; R)$ es un conjunto clasificado, entonces todo elemento de X pertenece a una única clase de equivalencia, lo cual, expresado en lenguaje lógico-matemático es:
si $(A; R)$ es un conjunto clasificado, entonces $(\forall x \in A)(\exists! a \in A)(x \in [a]_R)$.

Demostración.— Esta es una *demostración de existencia y de unicidad —cfr. supra* § 7.1 (pág. 466 de esta edición) y § 7.2 (pág. 467 de esta edición)—.

0. *Existencia*:
Veamos que $\forall a \in A$, existe al menos una clase de equivalencia a la que pertenece. En efecto, sea $[a]_R = \{x \in A : \langle x, a\rangle \in R\}$ y como R es una equivalencia, R es reflexiva, es decir, $(a, a) \in R$, de donde de la definición de $[a]_R$, se sigue que $a \in [a]_R$.

1. *Unicidad*:
Razonemos por reducción al absurdo. Sea $a \in A$ perteneciente a dos clases de equivalencia distintas, $[x]_R$ e $[y]_R$; vamos a demostrar que, entonces, $[x]_R = [y]_R$. Lo hacemos por doble inclusión. Veamos que $[x]_R \subseteq [y]_R$. En efecto, sea $t \in [x]_R$. Por un lado, por definición de clase de equivalencia, tRx, como $a \in [x]_R$, aRx, como R es de equivalencia, R es simétrica y transitiva, por ser simétrica, xRa y por ser transitiva $tRx \wedge xRa \rightarrow tRa$; por otro, como $a \in [y]_R$, aRy y, entonces, por transitividad de R, $tRa \wedge aRy \rightarrow tRy$, esto es, $t \in [y]_R$. De manera similar pudiésemos demostrar que $[y]_R \subseteq [x]_R$, por lo que se tiene la igualdad. De este modo, hemos deducido una fórmula insatisfactible, a saber, $([x]_R \neq [y]_R) \wedge ([x]_R = [y]_R)$,

[19] Alternativamente, $[a] = \{x \in \mathbb{Z} : a^2 - x^2 = a - x\} = \{x \in \mathbb{Z} : (a+x)(a-x) = a - x\} = \{a\} \cup \{x \in \mathbb{Z} \setminus \{a\} : a + x = 1\} = \{a\} \cup \{1 - a\}$.

por lo que por reducción al absurdo, es cierto que $a \in A \to a$ pertenece a una única clase de equivalencia. ■

Observación 11.22.3.— Esta demostración justifica la definición de relación de equivalencia. En la demostración hemos necesitado las tres exigencias, ser reflexiva, simétrica y transitiva, ni una más ni una menos.

Teorema 11.27
Si $(A; R)$ es un conjunto clasificado, entonces elementos de A equivalentes por R generan clases de equivalencia idénticas, lo cual, con signos lógico-matemáticos, es:
si $(A; R)$ es un conjunto clasificado, entonces $(\forall a, b \in A)(aRb \to [a]_R = [b]_R)$.

Demostración.— Demostremos que $[a]_R = [b]_R$ por doble inclusión.

$\subseteq$: $x \in [a]_R \to xRa$ y como aRb, por transitiva, xRb, de donde, $x \in [b]_R$, esto es, $[a]_R \subseteq [b]_R$.

$\supseteq$: $x \in [b]_R \to xRb$ y como bRa (por ser simétrica, de aRb), por transitiva, xRa, de donde, $x \in [a]_R$, esto es, $[a]_R \supseteq [b]_R$. ■

§ 11.22.1 Conjunto cociente y conjunto de representantes

Definición 11.41.— Sea $(X; R)$ un conjunto clasificado. Llamamos *conjunto cociente* de la relación R en X, y notamos X/R, al conjunto de todas las clases de equivalencia.

Ejemplo 335

Hallemos el conjunto cociente correspondiente al ejemplo 334 (pág. 631 de esta edición).

Resolución.— $\mathbb{Z}/R = \{[n] : n \in \mathbb{Z}\} = \{\{0, 1\}, \{-1, 2\}, \{-2, 3\}, \{-3, 4\}, \ldots, \{-n, n + 1\}, \ldots\}$. ■

Teorema 11.28
La familia de los representantes de las clases de equivalencia $\{x_{[x]_R}\}_{[x]_R \in X/R}$ es un *conjunto de representantes* de X —*vid. supra* definición 11.27 (pág. 613 de esta edición)—.

Ejemplo 336

Consideremos la relación R definida en $\mathbb{Z} \times \mathbb{Z}$ por, $\forall \langle x, y \rangle, \langle u, v \rangle \in \mathbb{Z} \times \mathbb{Z}$,

$$\langle x, y \rangle \, R \, \langle u, v \rangle \leftrightarrow x + v = y + u.$$

0. Demostremos que R es una relación de equivalencia en $\mathbb{Z} \times \mathbb{Z}$.
1. Determinemos el conjunto cociente $\mathbb{Z} \times \mathbb{Z} / R$ y representémoslo gráficamente.

[EFE 17.1.2022:3], [PEP 5.4.2022:3]. *Cfr.* García, Hernández y Nevot [150]: problema resuelto 4.11 (pág. 151).

Resolución.—

0. Veamos que es reflexiva, simétrica y transitiva.

   - R es reflexiva en $\mathbb{Z} \times \mathbb{Z}$; en efecto, $\forall \langle x, y \rangle \in \mathbb{Z} \times \mathbb{Z}$,

$$\begin{aligned} x + y &= y + x && \text{[conmutativa de } + \text{ en } \mathbb{Z}] \\ &\leftrightarrow \langle x, y \rangle \, R \, \langle x, y \rangle && \text{[definición de } R]; \end{aligned}$$

   - R es simétrica en $\mathbb{Z} \times \mathbb{Z}$; en efecto, $\forall \langle x, y \rangle, \langle u, v \rangle \in \mathbb{Z} \times \mathbb{Z}$,

$$\begin{aligned} \langle x, y \rangle \, R \, \langle u, v \rangle &\leftrightarrow x + v = y + u && \text{[definición de } R] \\ &\leftrightarrow u + y = v + x && \text{[conmutativa de } + \text{ en } \mathbb{Z}] \\ &\leftrightarrow \langle u, v \rangle \, R \, \langle x, y \rangle && \text{[definición de } R]; \end{aligned}$$

   - R es transitiva en $\mathbb{Z} \times \mathbb{Z}$; en efecto, $\forall \langle x, y \rangle, \langle u, v \rangle, \langle z, t \rangle \in \mathbb{Z} \times \mathbb{Z}$,

$$\begin{aligned} \langle x, y \rangle \, R \, \langle u, v \rangle &\leftrightarrow x + v = y + u && \text{[definición de } R] \\ \langle u, v \rangle \, R \, \langle z, t \rangle &\leftrightarrow u + t = v + z && \text{[definición de } R] \\ &\rightarrow x + v + u + t = y + u + v + z && \text{[sumando miembro a miembro]} \\ &\leftrightarrow (x + t) + (u + v) = (y + z) + (u + v) && \text{[conmutativa y asociativa de } + \text{ en } \mathbb{Z}] \\ &\leftrightarrow x + t = y + z && \text{[monotonía y cancelación de } + \text{ en } \mathbb{Z}] \\ &\leftrightarrow \langle x, y \rangle \, R \, \langle z, t \rangle. && \text{[definición de } R] \end{aligned}$$

1. Para todo $\langle a, b \rangle \in \mathbb{Z} \times \mathbb{Z}$,

$$\begin{aligned} [\langle a, b \rangle]_R &= \{\langle x, y \rangle \in \mathbb{Z} \times \mathbb{Z} : a + y = b + x\} && \text{[definición de } R \text{ y de clase de equivalencia]} \\ &= \{\langle x, y \rangle \in \mathbb{Z} \times \mathbb{Z} : y = x + (b - a)\} && \text{[aritmética en } (\mathbb{Z}, +, \cdot)], \end{aligned}$$

de donde, por ser a y b números enteros arbitrarios, el conjunto cociente ${}^{\mathbb{Z}\times\mathbb{Z}}\!/_{R}$ es el conjunto infinito numerable de rectas

$$ {}^{\mathbb{Z}\times\mathbb{Z}}\!/_{R} = \{y = x + n : n \in \mathbb{Z}\}, $$

en efecto, $\forall n \in \mathbb{Z}$,

- las clases $[\langle 0, 0\rangle]_R = [\langle -1, -1\rangle]_R = [\langle 1, 1\rangle]_R = [\langle -2, -2\rangle]_R = \cdots = [\langle -n, -n\rangle]_R = [\langle n, n\rangle]_R = \cdots$ son la recta $y = x$,
- las clases $[\langle -n, 0\rangle]_R = [\langle 0, n\rangle]_R$ son las rectas $y = x + n$,
- las clases $[\langle 0, -n\rangle]_R = [\langle n, 0\rangle]_R$ son las rectas $y = x - n$.

Vemos parte de su representación en la figura 11.5 (pág. 635 de esta edición).

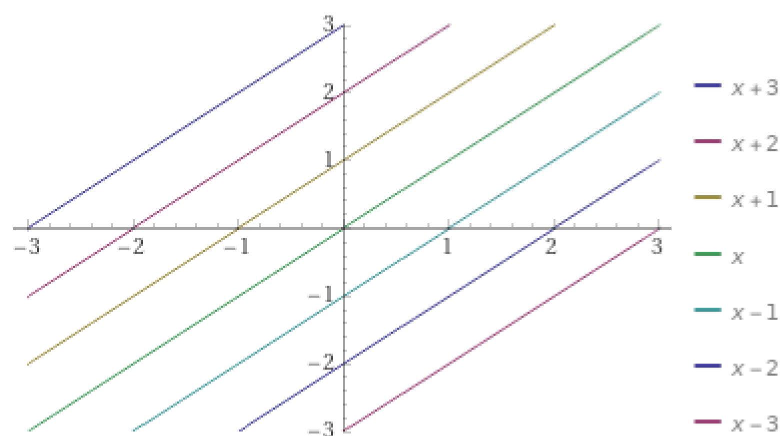


Figura 11.5.— Representación de siete de las clases de equivalencia —cuyo número es infinito numerable— de la relación de equivalencia analizada; el dibujo está generado con el artefacto en línea Wolfram|Alpha (https://www.wolframalpha.com) de Wolfram Research, con la entrada `plot y=x+3, y=x+2, y=x+1, y=x, y=x-1, y=x-2, y=x-3, -3 <= x <= 3, -3 <= y <= 3`.

■

Actividad 11.5

Sean $A = \{0, 1, 2, 3\}$ y la relación R definida en A por, $\forall x, y \in A$,

$$ x\,R\,y \leftrightarrow (x = y) \vee (x + y = 2). $$

0. Definamos R por extensión.
1. Demostremos que R es una relación de equivalencia en A.
2. Hallemos el conjunto cociente ${}^{A}\!/_{R}$.

[PEP 14.4.2023:3]. *Cfr.* Rojo [146]: trabajo práctico III 3.27 (págs. 99 y 428).

§ 11.22.2 Aplicación natural

Definición 11.42.— Sea $(X; R)$ un conjunto clasificado. Llamamos *aplicación natural* (o, sinónimamente, *aplicación canónica*) a la aplicación $\mathrm{n} : X \longrightarrow X/R$, definida en X por $\mathrm{n}(x) = [x]_R$, esto es, la imagen de cada elemento es su clase de equivalencia; en algunos textos se designa por π.

Ejemplo 337

Demostremos que la aplicación natural es, en efecto, una aplicación que, además, es sobreyectiva y no inyectiva.

Resolución.— En efecto,

0. el teorema 11.26 (pág. 632 de esta edición) demuestra que es aplicación;
1. el teorema 11.25 (pág. 631 de esta edición) demuestra que es sobreyectiva, y
2. el teorema 11.27 (pág. 633 de esta edición) demuestra que no es inyectiva. ∎

Definición 11.43.— Toda función $f : X \longrightarrow Y$ determina una relación de equivalencia $\sim_f$ en X, definida por $x \sim_f y$ si, y sólo si, $f(x) = f(y)$, esto es, si, y sólo si, $f(x) - f(y) = 0$ ($\sim_f$ es conocida como núcleo de f y usualmente se la designa por $\ker f$ —notemos que si f es una aplicación lineal, esta definición queda $x \sim_f y$ si, y sólo si, $f(x - y) = 0$ por lo que su núcleo puede describirse como el subespacio vectorial $\ker f = \{x \in X : f(x) = 0\}$—).

Teorema 11.29

Es posible descomponer f como $f = i \circ g \circ \mathrm{n}$:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow{\scriptstyle \mathrm{n}} & & \uparrow{\scriptstyle i} \\ X/\ker f & \xrightarrow{g} & f(X) \end{array}$$

donde:

- n es la aplicación natural, sobreyectiva, definida, como sabemos, por $\mathrm{n}(x) = [x]_{\ker f}$,
- g es la aplicación biyectiva definida por $g([x]_{\ker f}) = f(x)$, e
- i es $\mathrm{id}_{f(X)}$, la aplicación identidad en $f(X)$, esto es, la aplicación inyectiva definida por $i(x) = x$.

§ 11.23 Clasificar es particionar, y recíprocamente

Teorema 11.30
Si $(X; R)$ es un conjunto clasificado, entonces ${}^{X}/_{R}$, es una partición de X.

Es por esto por lo que decimos que R *clasifica* los elementos de X y que ${}^{X}/_{R}$ es una *clasificación* de X. De hecho, a las particiones también las denominamos clasificaciones.

Ejemplo 338

Estudiemos la *relación diádica* «ser del mismo color que» en el conjunto B de todas las bolas blandas de colores que llenan una piscina, siendo éstas de tres colores, rojo, verde y azul.

Resolución.— No es difícil demostrar que esta relación es de equivalencia en B. Imaginemos ahora que reunimos las bolas del mismo color en bolsas. Tenemos así la bolsa de bolas de color rojo, la bolsa de bolas de color verde y la bolsa de bolas de color azul. Elegimos una bola de cada bolsa y la adherimos por fuera con el objetivo de que cada bolsa quede identificada. Cada una de estas bolsas es una *clase de equivalencia* y la bola que la identifica su *representante canónico*. La reunión de las tres bolsas es el *conjunto cociente* de la relación. La colección de las tres bolas identificativas es un *conjunto de representantes*[20] de B. ■

Hemos visto cómo una relación de equivalencia determina una partición en un conjunto. Veamos ahora que el recíproco también es cierto, toda partición en un conjunto determina una relación de equivalencia en dicho conjunto.

Teorema 11.31
Sean X un conjunto no vacío y P una partición de X, entonces la relación R definida en X por

$$xRy \leftrightarrow (\exists S \in P)\,(x \in S \wedge y \in S),$$

para cualesquiera x, y de X, es una relación de equivalencia en X —cuyo conjunto cociente es P—.

En palabras llanas, tener una relación de equivalencia definida en un conjunto es tener una partición de éste y, recíprocamente, tener una partición de un conjunto es tener una relación de equivalencia en él.

[20] *Vid. supra* definición 11.27 (pág. 613 de esta edición).

Relaciones semánticas en un tesauro

Cuando elaboramos un tesauro* definimos naturalmente relaciones semánticas entre los términos contenidos en el mismo. Por una parte, la *relación entre sinónimos*, una relación de equivalencia en la que cada clase representa una colección de términos sinónimos, uno de los cuales elegimos como descriptor del concepto —en otras palabras, como el representante de la clase de equivalencia—, e interpretamos el resto de sinónimos —esto es, el resto de elementos de dicha clase de equivalencia— como términos alternativos asociados a dicho descriptor. Por otra, definimos *relaciones de asociación* entre términos, de dos tipos: bien una *relación de asociación débil*, cuando desde un término referenciamos otro pero no al revés, bien una *relación de asociación fuerte*, entre términos mutuamente referenciados. Un ejemplo de esta última es la propia relación entre sinónimos comentada anteriormente; otros son las *relaciones de jerarquía* que pudiesen existir y las *relaciones de traducción* en tesauros multi-idiomas. Por otra, relaciones de mayor grado de abstracción, por ejemplo *relaciones de analogía* entre metatérminos —argumentos, situaciones, etc.—. Todas estas relaciones son parte esencial de los algoritmos de búsqueda en tesauros y de los de lenguaje, razonamiento e inferencia que utilizan o incorporan a aquéllos.

* *Vid. v. gr.* https://en.wikipedia.org/wiki/Thesaurus_(information_retrieval); un ejemplo: SKOS, el tesauro de la UNESCO (https://skos.um.es/unescothes/?l=es).

§ 11.24 Relación de tolerancia

A una relación simétrica y reflexiva, a veces, se le llama relación de *tolerancia* (o, sinónimamente, *relación de compatibilidad* o *relación de cercanía*[21]. En ellas, al no exigir que sean transitivas, se permite que un elemento sea clasificado en más de una clase. En determinados ámbitos, a una relación de tolerancia transitiva, esto es, a una equivalencia, se la conoce como *relación de indiscernibilidad*.

Definición 11.44.— Sean X un conjunto y R una relación diádica en X. Decimos que R es una relación de:

- *tolerancia* en X si, y sólo si, R es reflexiva y simétrica en X;
- *dependencia* en X si, y sólo si, X es un conjunto finito.

Definición 11.45.— Sean un conjunto no vacío X y una relación de tolerancia R en X. Llamamos *clase de tolerancia* (o, sinónimamente, *conjunto de elementos compatibles/parecidos/semejantes/similares*) a

[21] Una relación diádica reflexiva y simétrica, a veces aparece en la literatura con el nombre de (relación de) *parecido*. Claro que también nos la encontramos con el nombre de *semejanza* —*cfr. v. gr.* Kaufmann, Dubois y Cools [163] (pág. 34, de la edición española). También apareció con el nombre de *similitud* en la tesis doctoral de quien escribe, León Rojas [1] (definición 48, pág. 95).

todo subconjunto S de X tal que $\forall x, y \in S, xRy$ (comparemos esta definición con la de clase de equivalencia[22]).

Observación 11.24.0.— El conjunto vacío es una clase de tolerancia, ya que $\forall x, y \in \emptyset, xRy$ es verdadero (por vacuidad).

Definición 11.46.— Llamamos *clase maximal de tolerancia* a toda clase de tolerancia que no está contenida en ninguna otra clase de tolerancia.

Observación 11.24.1.—

- En algunos textos las clases de tolerancia y las clases maximales de tolerancia aparecen denominadas como preclases de tolerancia y clases de tolerancia —preclases maximales—, respectivamente.
- Pensemos que diversas relaciones de parecido, semejanza, proximidad, amistad, vecindad, grupales, gremiales, podrían modelizarse como relaciones de tolerancia —siempre que admitamos que son reflexivas; a modo de ejemplo, que toda persona es amiga de sí misma—.

Definición 11.47.— Llamamos *espacio de tolerancia* al conjunto de todas las clases maximales de tolerancia.

Teorema 11.32
Dada una relación de tolerancia R en un conjunto no vacío X, el espacio de tolerancia es un recubrimiento de X.

Teorema 11.33
Dado un recubrimiento C de un conjunto no vacío X, entonces la relación R definida en X por

$$(\forall x, y \in X)(xRy \leftrightarrow (\exists S \in C)\,(x \in S \wedge y \in S)),$$

es una relación de tolerancia en X (cuyo espacio de tolerancia es C).

Observación 11.24.2.—

- Como toda partición es un recubrimiento, todo conjunto cociente es un espacio de tolerancia.
- Como no todo recubrimiento es una partición, no todo espacio de tolerancia es un conjunto cociente.

Observación 11.24.3.— La intersección de dos clases de tolerancia/compatibilidad pudiese interpretarse como una zona común de *influencia* de los respectivos elementos definidores de dichas clases; por ejemplo, si dados dos números x, y, $xRy \leftrightarrow |x - y| < 2$, como $[n] = \{n-1, n, n+1\}$ y

[22] *Vid. supra* definición 11.40 (pág. 630 de esta edición).

$[n+2] = \{n+1, n+2, n+3\}$, la zona común de influencia de n y $n+2$ es $\{n+1\}$, esto es, bien pudiésemos decir que la influencia sobre $n+1$ de n y de $n+2$ es la misma.[23]

Definición 11.48 (Métrica de Hamming).— Dadas dos palabras finitas $x = x_0x_1\dots x_{p-1}$ e $= y_0y_1\dots y_{q-1}$, de longitudes $|x| = p$ e $|y| = q$, la distancia de Hamming entre ellas viene dada por

$$d_H(x,y) \leftrightharpoons |\{i \in \{0,\dots,\min(p-1,q-1) : m_i \neq n_i\}\}| + \max(p,q) - \min(p,q).$$

La distancia de Hamming es una métrica[24]. Si $|x| = |y|$, esto es, si x e y son de la misma longitud, la distancia de Hamming entre ellas es el número de posiciones en las que los símbolos correspondientes son diferentes.

Ejemplo 339

Sea C un conjunto de palabras. Sea R la relación diádica definida en C por

$$xRy \leftrightarrow d_H(x,y) \leq 3.$$

0. Estudiemos si R satisface o no las propiedades reflexiva, simétrica, antisimétrica, transitiva y conexa (fuertemente completa) y digamos qué tipo de relación es y por qué lo es.
1. Proporcionemos un ejemplo de conjunto C y considerando R actuando en él, hallemos, bien las clases de tolerancia y las clases maximales de tolerancia, bien las clases de equivalencia, bien dibujemos un diagrama de Hasse, dependiendo de que R sea, respectivamente, una relación de tolerancia, una relación de equivalencia o una ordenación en C.

[AIC 10.4.2019:2b], [EFO 20.5.2022:3], [EFE 28.6.2023:3].

Resolución.—

0. 1. Dadas cualesquiera tres palabras finitas de igual longitud, x, y, z, entonces:

    0. $d_H(x,x) = 0$ pues cuando comparamos x con x los símbolos son iguales en todas las posiciones y como $0 \leq 3$, se tiene que R es reflexiva;

[23] Acercando esta interpretación a la lógica borrosa, en concreto a los números borrosos, pudiésemos decir que $n+1$ es tan n como $n+2$.

[24] *Cfr. supra* definición 10.24 (pág. 565 de esta edición).

1. $d_H(x, y)$ denota el número de posiciones en los que los símbolos correspondientes en las dos palabras son distintos, pero esto da igual tener x y comparar con y que tener y y comparar con x, esto es, $d_H(x, y) = d_H(y, x)$, por lo que si uno es menor o igual que tres, el otro, que es el mismo, también, luego R es simétrica;

2. no es antisimétrica, pues es posible proporcionar un contraejemplo, por ejemplo, si x es la palabra 0 e y la palabra 1, $d_H(x, y) = d_H(y, x) = 1 \leq 3$, por lo que xRy e yRx, y sin embargo, $x \neq y$;

3. tampoco es transitiva, pues, por ejemplo, si x, y y z son las palabras 0000, 0111 y 1111, respectivamente, se tiene que $d_H(x, y) = 3 \leq 3$ y, por tanto, que xRy, y que $d_H(y, z) = 1 \leq 3$ y, por tanto, que yRz; sin embargo, $d_H(x, z) = 4 \nleq 3$, esto es, que $x \neg Rz$, y

4. finalmente, no es conexa (fuertemente completa) ya que como sobre los elementos de C sólo sabemos que son palabras, pudiese haber palabras cuya distancia de Hamming fuese mayor que 3, y que, por tanto, no estuviesen relacionadas (por ejemplo, las palabras 0000 y 1111, cuya distancia de Hamming es 4), y también pudiese haber palabras no finitas o de longitudes diferentes, que tampoco estarían relacionadas.

II. Se trata de una relación de tolerancia, esto es, una relación simétrica y reflexiva.

1. La relación R actuando en $C = \{0000, 0111, 1111\}$ induce las siguientes *clases de tolerancia*: $\emptyset$, $\{0000\}$, $\{0111\}$, $\{1111\}$, $\{0000, 0111\}$ y $\{0111, 1111\}$. Dos de ellas no están contenidas en ninguna otra clase de tolerancia —la razón la expusimos anteriormente en la discusión de la transitiva—, son las *clases maximales de tolerancia*: $\{0000, 0111\}$ y $\{0111, 1111\}$. Su conjunto, $\{\{0000, 0111\}, \{0111, 1111\}\}$, es el *espacio de tolerancia* de R que, por cierto, es un *recubrimiento* de C. ■

Observación 11.24.4.— Que una relación sea simétrica no implica que no sea antisimétrica (ni que fuese antisimétrica implicaría que no fuese simétrica). Por ejemplo, además del ejemplo trivial de la relación vacía, simétrica y antisimétrica a la vez, si S es la relación de igualdad en $\mathbb{Z}$, esto es, $S = \{\langle x, y\rangle \in \mathbb{Z}^2 : x = y\}$, entonces cualquier subconjunto de S, es decir, cualquier elemento de su conjunto potencia 2^S, es una relación simétrica y antisimétrica en $\mathbb{Z}$.

§ 11.25 Clausuras

¿Cómo pudiésemos completar una relación de tolerancia para que fuese transitiva, esto es, para que fuese una relación de equivalencia?

Además, ¿cómo pudiésemos hacerlo para que encontrásemos la menor —respecto de la inclusión de conjuntos— relación de equivalencia que contiene a una relación de tolerancia dada?

Aún más, ¿cuál es la menor relación de tolerancia que incluye a una relación dada? ¿Y la menor relación de equivalencia?

Este hecho de completar una relación diádica en un conjunto que no satisfaga una o varias determinadas propiedades de forma que acabe satisfaciéndolas se llama *cerrar o clausurar la relación* para esas propiedades.

Definición 11.49.— Supongamos que una relación R definida en un conjunto X pueda satisfacer o no una determinada propiedad P. Si existe una relación S definida en X que satisface la propiedad P, que contiene a R y que es subconjunto de cualquier relación que satisfaga P y que contenga a R, entonces decimos que S es el cierre o *clausura de R respecto de P* . En definitiva, si genéricamente $\operatorname{cl}_P R$ la designa y si $S \subseteq X \times X$, entonces

$$S = \operatorname{cl}_P R \ \leftrightharpoons PS \wedge (R \subseteq S) \wedge ((\forall S' \subseteq X \times X)(PS' \wedge R \subseteq S') \rightarrow S \subseteq S').$$

Teorema 11.34

Se satisface:

0. S es la *clausura reflexiva* de $R \subseteq X^2$ si, y sólo si, $S = R \cup \{\langle x, x\rangle : x \in X\}$, esto es, precisamente si $S = R \cup I_X$ —es decir, para hallar la clausura reflexiva de una relación basta añadirle los pares ordenados de componentes iguales—; notamos la clausura reflexiva de R por $R^{=}$;
1. S es la *clausura simétrica* de $R \subseteq X^2$ si, y sólo si, $S = R \cup \{\langle y, x\rangle : \langle x, y\rangle \in R\}$, esto es, precisamente si $S = R \cup R^{-1}$; notamos la clausura simétrica de R por $R^{\leftrightarrow}$ o $R^{\sim}$;
2. R^{+} es la *clausura transitiva* de $R \subseteq X^2$ si, y sólo si, $R^{+} = \bigcup_{i \in \mathbb{Z}^{+}} R^i$, siendo $R^1 = R$ y $\forall i \in \mathbb{Z}^{+}$, $R^{i+1} = R^i \circ R$ —si $|X| = n$, $R^{+} = \bigcup_{i=1}^{n} R^i$—.

Observación 11.25.0.— Notemos que como corolario del teorema anterior se definen nuevas clausuras y se satisface:

0. $I_X \cup R \cup R^{-1}$ es *la clausura reflexiva y simétrica* de R, que notamos abreviadamente por $R^{\simeq}$; se satisface que $R^{\simeq} = (R^{=})^{\sim} = (R^{\sim})^{=}$; en el sentido de la inclusión de conjuntos, *es la menor relación de tolerancia que contiene a R*;
1. $I_X \cup R^{+}$ es *la clausura reflexiva y transitiva* de R —designando I_X por R^0, la clausura reflexiva y transitiva es $\bigcup_{i \in \mathbb{N}} R^i$ que abreviamos $R^{+}_{\circ}$ (en determinados entornos también se nota R^*)—; se satisface que $R^{+}_{\circ} = (R^{+})^{=} = (R^{=})^{+}$; en el sentido de la inclusión de conjuntos, *es la menor relación de preorden parcial que contiene a R*;

2. $R^+ \cup R^{-1}$ es *la clausura simétrica y transitiva* de R; a veces, se nota R^{PER} o R^{EQ}; se satisface que $R^{\mathrm{PER}} = (R^{\sim})^+ = (R^+)^{\sim}$; en el sentido de la inclusión de conjuntos, es *la menor relación de equivalencia parcial que contiene a* R;

3. $I_X \cup R^+ \cup R^{-1}$ es *la clausura reflexiva, simétrica y transitiva* de R; se nota $R^{\equiv}$ o R^{EQV}; se satisface que $R^{\equiv} = (R^{\simeq})^+ = (R_0^+)^{\sim} = (R^{\mathrm{PER}})^{=}$; en el sentido de la inclusión de conjuntos, es *la menor relación de equivalencia que contiene a* R.

Recordemos que la relación unión de dos relaciones transitivas no tiene por qué ser una relación transitiva. Como comentábamos, este resultado implica, en particular, que la relación unión de dos relaciones de equivalencia no tiene por qué ser de equivalencia. Así, por ejemplo, *para obtener una relación de equivalencia a partir de la unión de dos relaciones de equivalencia*, un camino consistiría en hallar su unión y calcular la clausura transitiva de dicha relación unión; tal clausura es una relación de equivalencia, además, es la menor en el sentido de la inclusión de conjuntos.

Ejemplo 340

Sea $X = \{0, 1, 2\}$ y sean $\sim_0$ y $\sim_1$ dos relaciones de equivalencia definidas en X tales que $[0]_{\sim_0} = \{0, 1\} = [1]_{\sim_0}$, $[2]_{\sim_0} = \{2\}$, $[0]_{\sim_1} = \{0\}$ y $[1]_{\sim_1} = \{1, 2\} = [2]_{\sim_1}$.

0. Demostremos que $R = \sim_0 \cup \sim_1$ no es una relación de equivalencia.
1. Hallemos la relación de equivalencia más pequeña —en el sentido de la inclusión de conjuntos— que incluye a ambas relaciones.

Resolución.— En efecto,

0. se tiene que $0 \sim_0 1$ y $1 \sim_1 2$, por lo que, por definición de unión, $0R1$ y $1R2$; sin embargo, como $0 \nsim_0 2$ y $0 \nsim_1 2$, igualmente por definición de unión, $0 \neg R\, 2$, por lo que no es transitiva y por tanto, no es de equivalencia;

1. construyamos la clausura transitiva de R:

   I. $\sim_0 = \{\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 1, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle\}$,

   II. $\sim_1 = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$,

   III. $R^1 = R = \sim_0 \cup \sim_1 = \{\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 1, 0\rangle, \langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$,

   IV. $R^2 = R^1 \circ R = R \circ R = \{\langle x, z\rangle \in X \times X : (\exists y \in X)(xRy \wedge yRz)\} = \{\langle 0, 0\rangle, \langle 0, 1\rangle, \langle 0, 2\rangle, \langle 1, 0\rangle, \langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 0\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$[25].

   Aunque el algoritmo de cálculo de la clausura transitiva[26] dice que si $|X| = 3$, $R^+ = R^1 \cup R^2 \cup R^3$, con $R^3 = R^2 \circ R$, nos damos cuenta de que R^2 tiene $9 = 3^2$ elementos y éste es precisamente el

[25] $\langle 0, 2\rangle \in R^2$ porque $\langle 0, 1\rangle \in R^2$ y $\langle 1, 2\rangle \in R^2$; $\langle 2, 0\rangle \in R^2$ porque $\langle 2, 1\rangle \in R^2$ y $\langle 1, 0\rangle \in R^2$.
[26] *Vid.* apartado c) del teorema 11.34 (pág. 642 de esta edición).

número de variaciones con repetición de 3 elementos —los de X— tomados de 2 en 2; en otras palabras, no existen más parejas, en R^2 están todas las posibles; por tanto, terminamos la ejecución de dicho algoritmo, obteniendo que la clausura transitiva de R es $R^+ = R^1 \cup R^2 = R^2$, es decir, que la relación de equivalencia que buscábamos es R^2. ■

Para finalizar, en el caso de la clausura transitiva, no nos olvidemos, por su interés computacional, de los algoritmos[27] para calcularla, por ejemplo, el algoritmo de FLOYD y WARSHALL[28].

§ 11.26 Ordenaciones

Afirman que la esencia de la ordenación es la transitividad; otras personas insisten en que lo es conjuntamente con la asimetría. Por ejemplo, GALINDO [164] (pág. 58) llama una estructura de *orden parcial* a un conjunto X, no vacío, entre alguno de cuyos pares de elementos se de una relación diádica que sea *asimétrica* y *transitiva*, y en la que hay efectivamente pares de elementos *incomparables*, esto es, $(\exists x, y \in X)(x \not\preceq y \wedge y \not\preceq x)$. Sitúan esta estructura como el eje de las discusiones e insisten: si adjetivamos parcial al orden, existen elementos incomparables.

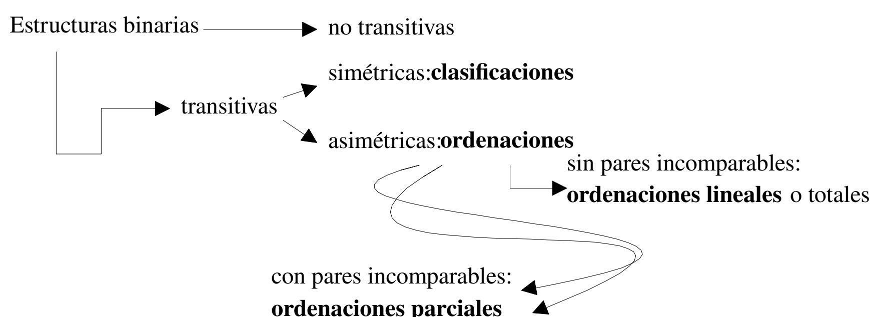


Figura 11.6.— Principales estructuras diádicas. En un principio, la reflexividad carece de importancia (ver texto). Quizás nos llame la atención que las flechas desde ordenaciones a ordenaciones parciales se cruzan dos veces. Con ello queremos plasmar gráficamente la existencia de *pares incomparables*. Lo único que hemos de hacer es ver cada flecha como una ordenación fuertemente completa.

En principio, el ser reflexiva —$(\forall x \in X)(x \preceq x)$—, o no serlo, puede parecer que carece de importancia —*cfr.* figura 11.6 (pág. 644 de esta edición). No obstante, puede que como sentencia MENGER en la primera página de *Kurventheorie* [165]: «lo que afirma la intuición no debe negarlo el concepto» y «lo que niega la intuición no debe afirmarlo el concepto» , y hay múltiples ejemplos en los que la necesidad de la reflexividad es patente. Uno clásico es la ordenación cronológica de los puntos de un recorrido cíclico, donde cada punto es precedido en el tiempo por él mismo: por ejemplo, las 17 horas de hoy preceden a las 17 horas de mañana (pero no deja de ser el mismo número, 17). Otro proviene

[27] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Transitive_closure#Algorithms.
[28] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Floyd-Warshall_algorithm.

de nuestra intuición de semejanza: lo muy semejante ha de ser muy poco diferente. Esto significa la tendencia a la reflexividad en el límite hacia la semejanza máxima.

Lo que sí es usual es utilizar el adjetivo *estricto* para un orden e impedir su reflexividad. Se denota por el símbolo $\prec$. A la par, han surgido nombres como *preorden* o *casi orden* para la estructura que verifica la reflexividad y la transitividad (aunque dada la poca significación de la reflexividad, puede parecer pecar de ampulosa).

Observación 11.26.0.— No sobra que leamos la opinión crítica de Galindo al baturrillo de nombres existente en torno a las estructuras diádicas en su trabajo de grado de licenciatura [164] (cap. 3). Tampoco está de más consultar la obra de Cuesta Dutari [166].

§ 11.26.0 Preorden

Dicho lo anterior, resta mencionar que en la actualidad son comunes las siguientes definiciones.

Definición 11.50.— Sean X un conjunto y $\preceq$ una relación diádica en X. Decimos que $\preceq$ es una relación de *preorden parcial* (o *casi orden*) en X precisamente si $\preceq$ es transitiva y reflexiva en X. Decimos entonces que X es un conjunto parcialmente preordenado por $\preceq$ (o, sinónimamente, que $(C; \preceq)$ es un *conjunto parcialmente preordenado*).

Ejemplo 341

0. $(\{0, 1\}, \preceq)$, con $\preceq = \{\langle 0, 0\rangle, \langle 1, 1\rangle\}$, es un conjunto parcialmente preordenado;
1. $(\{0, 1\}, \preceq)$, con $\preceq = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 0, 1\rangle\}$, es un conjunto parcialmente preordenado;
2. $(\{0, 1, 2\}, \preceq)$, con $\preceq = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 0, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle\}$, no es un conjunto parcialmente preordenado, ya que $\preceq$ no es transitiva en $(\{0, 1, 2\}$ pues $(0 \preceq 1) \wedge (1 \preceq 2) \wedge (0 \not\preceq 2)$.

Definición 11.51.— Sean X un conjunto y $\preceq$ una relación diádica en X. Decimos que $\preceq$ es una relación de *preorden* (u *orden débil*) en X precisamente si $\preceq$ es una relación de preorden parcial fuertemente completa en X (es decir, una relación transitiva, reflexiva y fuertemente completa en X). Decimos entonces que X es un conjunto preordenado por $\preceq$ (o, sinónimamente, que $(X; \preceq)$ es un *conjunto preordenado*).

Ejemplo 342

$(\{0, 1, 2\}, \preceq)$, con $\preceq = \{\langle 0, 0\rangle, \langle 1, 1\rangle, \langle 2, 2\rangle, \langle 0, 1\rangle\}$, es un conjunto parcialmente preordenado pero no es un conjunto preordenado, ya que $\preceq$ no es fuertemente completa en $(\{0, 1, 2\}$ pues, por ejemplo, ni $0 \preceq 2$ ni $2 \preceq 0$.

Observación 11.26.1.— Como la compleción fuerte implica la reflexividad, puede definirse una relación de preorden como aquélla que es transitiva y fuertemente completa.

Preorden asociado a una disimilaridad

Dado un conjunto finito de entidades $\Omega = \{0, 1, \ldots, n\}$, podemos definir un preorden $\preceq$ asociado a una disimilaridad d entre entidades como una relación diádica en $\Omega \times \Omega$, definida $\forall \langle i, j \rangle \in \Omega \times \Omega$ por $\langle i, j \rangle \preceq \langle i', j' \rangle$ si, y sólo si, $d(i, j) \leq d(i', j')$. El análisis de proximidades* (*multidimensional scaling*, MDS) es un método de Análisis Multivariante —utilizado, por ejemplo, en Política para cuantificar la similaridad entre naciones de acuerdo a un conjunto de dimensiones políticas, sociales y geográficas— que utiliza este tipo de preordenaciones.

* *Cfr. v. gr.* Shepard [167] y [168], y Kruskal [169] y [170].

§ 11.26.1 Orden parcial

Definición 11.52.— Sean X un conjunto y $\preceq$ una relación diádica en X. Decimos que $\preceq$ es una relación de *orden parcial* (o, sinónimamente, *orden débil*) en X precisamente si $\preceq$ es una relación de preorden parcial antisimétrica en X (es decir, una relación transitiva, reflexiva y antisimétrica en X). Decimos entonces que X es un conjunto ordenado parcialmente por $\preceq$ (o, sinónimamente, que $(X; \preceq)$ es un *conjunto parcialmente ordenado* (abreviadamente, *copo*)).

Ejemplo 343

Se satisface que:

0. $(2^A; \subseteq)$ es un conjunto parcialmente ordenado;
1. $(\mathbb{N}; \leq)$, $(\mathbb{Z}; \leq)$, $(\mathbb{Q}; \leq)$ y $(\mathbb{R}; \leq)$, con $\leq$ el orden habitual, son conjuntos parcialmente ordenados;
2. $(\mathbb{N}; |)$ es un conjunto parcialmente ordenado ($|$ es la relación de divisibilidad);
3. $(\mathbb{Z}; |)$ no es un conjunto parcialmente ordenado;
4. $(\mathbb{N}; =)$ es un conjunto parcialmente ordenado.

Definición 11.53.— Dados $(X; \preceq_X)$ y $(Y; \preceq_Y)$ dos conjuntos parcialmente ordenados, dos ordenaciones habituales del producto cartesiano $X \times Y$ vienen dadas por $\forall x, z \in X, \forall y, t \in Y$,

$$\textit{Orden producto}: \langle x, y \rangle \preceq_{\text{prod}} \langle z, t \rangle \leftrightarrow (x \preceq_X z \wedge y \preceq_Y t)$$
$$\textit{Orden lexicográfico}: \langle x, y \rangle \preceq_{\text{lex}} \langle z, t \rangle \leftrightarrow (x \prec_X z \vee (x = z \wedge y \preceq_Y t))$$

Ejemplo 344

Se satisface que $(X \times Y; \preceq_{\text{prod}})$ y $(X \times Y; \preceq_{\text{lex}})$ son conjuntos parcialmente ordenados.

Por lo general, en un conjunto preordenado $(X; \preceq)$ no se satisface la antisimétrica, es decir, puede suceder que $\exists x, y \in X$ tales que $x \preceq y$ e $y \preceq x$, siendo $x \neq y$.

Ejemplo 345

El conjunto preordenado $(\{0,1\}; \preceq)$, siendo $\preceq = \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 0,1\rangle, \langle 1,0\rangle\}$, no es un conjunto parcialmente ordenado.

Resolución.— $\preceq$ no es antisimétrica en $\{0,1\}$ pues $(0 \preceq 1) \wedge (1 \preceq 0) \wedge (0 \neq 1)$. ■

Actividad 11.6

El conjunto preordenado $(\Sigma^*; \preceq_{\text{long}})$, donde Σ^* es el conjunto de todas las palabras (palabras finitas, incluida la palabra vacía ϵ) formadas con letras de un alfabeto Σ y la relación diádica $\preceq_{\text{long}}$ está definida en Σ^* por

$$(\forall s_1, s_2 \in \Sigma^*) \big(s_1 \preceq_{\text{long}} s_2 \leftrightarrow \text{long}(s_1) \leq \text{long}(s_2)\big)$$

no es un conjunto parcialmente ordenado.

§ 11.26.2 Orden parcial estricto

Definición 11.54.— Sea un conjunto no vacío X y una relación diádica $\prec$ en X. Decimos que $\prec$ es una relación de *orden parcial estricto* (o, sinónimamente, *orden fuerte*) en X precisamente si $\prec$ es transitiva e irreflexiva en X (o, equivalentemente, si, y sólo si, $\prec$ es transitiva y asimétrica en X). Pudiésemos decir entonces, aunque no es habitual, que X es un conjunto estricta y parcialmente ordenado por $\prec$ (o, sinónimamente, que $(X; \prec)$ es un *conjunto estricta y parcialmente ordenado*).

Ejemplo 346

La relación $\prec = \{\langle 0,1\rangle, \langle 1,2\rangle, \langle 0,2\rangle\}$ es un orden parcial estricto en $\{0,1,2\}$ (notemos que como $\not\prec = \{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle, \langle 1,0\rangle, \langle 2,0\rangle, \langle 2,1\rangle\}$ es transitiva, $\prec$ es negativamente transitiva).

Definición 11.55.— Sea un conjunto no vacío X y una relación diádica $\prec$ en X. Decimos que $\prec$ es una relación de *orden débil estricto* en X precisamente si $\prec$ es negativamente transitiva y asimétrica en X. Pudiésemos decir entonces, aunque no es habitual, que X es un conjunto estricta y débilmente ordenado por $\prec$ (o, sinónimamente, que $(X; \prec)$ es un *conjunto estricta y débilmente ordenado*).

Observación 11.26.2.— En cuanto a ordenaciones, hemos de notar lo siguiente.

0. Se satisface que si $(X; \preceq)$ es un conjunto ordenado parcialmente y se define la relación diádica $\prec$ en X por

$$(\forall x, y \in X)\, (x \prec y \leftrightarrow (x \preceq y) \land \neg(y \preceq x)),$$

entonces $\prec$ es un orden parcial estricto en X.

1. Notemos que como toda relación transitiva es asimétrica si, y sólo si, es irreflexiva, también pudiésemos definir un orden parcial estricto en X como una relación irreflexiva y transitiva en X. Por otro lado, como ser asimétrica implica ser irreflexiva y antisimétrica, todo orden parcial estricto es una relación irreflexiva, antisimétrica y transitiva.

§ 11.26.3 Orden total

Definición 11.56.— Sea un conjunto X y una relación diádica $\prec$ en X. Decimos que $\prec$ es una relación de *orden total* (o, sinónimamente, *orden lineal*) en X precisamente si $\prec$ es una relación de orden parcial fuertemente completa (es decir, una relación transitiva, reflexiva, antisimétrica y fuertemente completa).

Ejemplo 347

Se satisface que:

0. $(2^A; \subseteq)$ es un conjunto totalmente ordenado;
1. $(\mathbb{N}; \leq)$, $(\mathbb{Z}; \leq)$, $(\mathbb{Q}; \leq)$ y $(\mathbb{R}; \leq)$, con $\leq$ el orden habitual, son conjuntos totalmente ordenados;
2. $(\mathbb{N}; \mid)$ no es un conjunto totalmente ordenado;
3. $(\mathbb{N}; =)$ no es un conjunto totalmente ordenado;
4. $\forall n \in \mathbb{N}$, $(\{n\}; =)$ es un conjunto totalmente ordenado;
5. $(A \times B; \preceq_{\text{lex}})$ es un conjunto totalmente ordenado, pero $(A \times B; \preceq_{\text{prod}})$ no lo es.

Observación 11.26.3.— La notación habitual para un orden es $\leq$, y para un orden estricto $<$; en cualquier caso, dado un conjunto ordenado $(X, \leq)$, cuando para dos elementos de X escribimos $x < y$, debemos entender que x está relacionado con x ($x \leq y$) siendo $x \neq y$; si escribimos $x \geq y$, debemos entender que $y \leq x$ y si escribimos $x > y$ que $y < x$. La afirmación $x \leq y$ la leemos x es *anterior* a y (o, sinónimamente, y es *posterior* a x) (en algunos textos encontramos x es *descendiente* de y —o, sinónimamente, y es *ascendiente* de x—). La afirmación $x < y$ la leemos x es *anterior estricto* a y. Caso de que $x < y$ y no exista $z \in A$ tal que $x < z < y$ tenemos que x es el *anterior directo/inmediato* de y (su *descendiente directo/inmediato*).

La tabla siguiente muestra los nombres de algunos tipos de ordenaciones frecuentes, según las propiedades que las definen de entre las vistas en este capítulo.

Relación\Propiedad	*R*	*I*	*S*	*A*	*An*	*T*	*nT*	*C*	*Cf*	*Fe*	*St*
Preorden parcial (casi orden)	✓					✓					
Preorden (orden débil)						✓			✓		
Preorden estricto				✓			✓				
Orden parcial	✓				✓	✓					
Orden parcial estricto				✓		✓					
Orden lineal					✓	✓			✓		
Orden lineal estricto				✓		✓		✓			
Orden de intervalos									✓	✓	
Orden estricto de intervalos		✓								✓	
Semiorden									✓	✓	✓
Semiorden estricto		✓								✓	✓

Cuadro 11.1.— Diferentes nombres de ordenaciones, según las propiedades que satisfacen. El significado de las abreviaturas figura en las definiciones de este capítulo. En algunos otros textos estas relaciones se definen atendiendo a otras propiedades, debido a equivalencias entre ellas; a modo de ejemplos: primero, como toda relación transitiva es asimétrica si, y sólo si, es irreflexiva, también es posible definir un orden parcial estricto en un conjunto, como una relación irreflexiva y transitiva en él, y segundo, un orden lineal estricto es una relación asimétrica, negativamente transitiva y completa. Se conoce mucho sobre todas estas relaciones; por ejemplo, notando $\preceq$ por $\precsim$ para evitar la confusión con la relación de igualdad: si $\precsim$ es un preorden lineal, entonces, la «parte» $\prec$ es un preorden y la parte $\sim$ es una equivalencia; si $\precsim$ es un orden lineal, entonces, $\prec$ es un orden lineal estricto; si $\precsim$ es un orden de intervalos, entonces, $\prec$ es transitiva; etc.

Actividad 11.7

Que en el cuadro aparezca un orden lineal como aquella relación que es antisimétrica, transitiva y fuertemente completa, no es una errata. Demostremos que el hecho de satisfacer esta tríada de propiedades obliga a que también sea reflexiva.

Ejemplo 348

0. Escribamos todas las relaciones diádicas que pueden definirse en el conjunto $\{0, 1\}$.
1. De todas las relaciones diádicas que pueden definirse en $\{0, 1\}$:
   a. ¿cuáles son de orden?;
   b. ¿cuáles son de orden total?;
   c. ¿cuáles son de equivalencia?;
   d. para las que sean de equivalencia, ¿cuáles son sus clases de equivalencia y sus conjuntos cocientes?

[Cubit 71], [EFO 4.6.2021:3].

Resolución.—

0. Por definición, una relación diádica en $\{0,1\}$ es cualquier subconjunto del producto cartesiano $\{0,1\} \times \{0,1\}$. Éste es un conjunto de cardinal 4; en efecto, $\{0,1\} \times \{0,1\} = \{(0,0),(0,1),(1,0),(1,1)\}$. El conjunto potencia de $\{0,1\} \times \{0,1\}$ tiene, por tanto, $2^4 = 16$ elementos que, por definición de relación diádica, como hemos dicho, son las relaciones diádicas buscadas (ya que nos serán de ayuda, escribimos también sus representaciones como matrices lógicas —booleanas—):

$$R_0 = \emptyset \qquad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$R_1 = \{(0,0)\} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$R_2 = \{(0,1)\} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$$R_3 = \{(1,0)\} \qquad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

$$R_4 = \{(1,1)\} \qquad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$R_5 = \{(0,0),(0,1)\} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

$$R_6 = \{(0,0),(1,0)\} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

$$R_7 = \{(0,0),(1,1)\} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$R_8 = \{(0,1),(1,0)\} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$R_9 = \{(0,1), (1,1)\} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$$

$$R_{10} = \{(1,0), (1,1)\} \qquad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

$$R_{11} = \{(0,0), (0,1), (1,0)\} \qquad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

$$R_{12} = \{(0,0), (0,1), (1,1)\} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$R_{13} = \{(0,0), (1,0), (1,1)\} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$R_{14} = \{(0,1), (1,0), (1,1)\} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$R_{15} = \{(0,0), (0,1), (1,0), (1,1)\} \qquad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

1. Para discutir si son de orden parcial, total o de equivalencia, es necesario saber si satisfacen las propiedades de reflexividad, simetría, antisimetría, transitividad y conexión (completitud fuerte). Para ello utilizaremos sus representaciones como matrices lógicas. Recordemos, dada una relación diádica $R \subseteq X \times X$ y su representación M como matriz lógica, R satisface en X la propiedad:

   - reflexiva si, y sólo si, $\mathrm{id}_X \subseteq R$, es decir, si, y sólo si, M tiene toda la diagonal principal 1 (esto es, si, y sólo si, $m_{ii} = 1$, para todo i);
   - simétrica si, y sólo si, $R \subseteq R^{-1}$, es decir, si, y sólo si, M es simétrica (esto es, si, y sólo si, $m_{ij} = m_{ji}$, para todo i, j);
   - antisimétrica si, y sólo si, $R \cap R^{-1} \subseteq \mathrm{id}_X$, es decir, si, y sólo si, los únicos elementos tales que $mij = m_{ji} = 1$ (o equivalentemente, $m_{ij} \cdot m_{ji} = 1$) están en la diagonal principal;
   - transitiva si, y sólo si, $R \circ R \subseteq R$, es decir, si, y sólo si, M^2 no tiene elementos no nulos donde M tenía elementos nulos, en otras palabras, $M - M^2 \geq 0$;
   - conexa (fuertemente completa) si, y sólo si, $R^\complement \subseteq R^{-1}$, esto es, si, y sólo si, $M^T - M^\complement \geq 0$, donde M^T es la traspuesta de M y $M^\complement$ se construye a partir de M intercambiando los ceros con los unos.

   De este modo, de todas las relaciones diádicas que pueden definirse en $\{0,1\}$, es decir, de las listadas en el apartado anterior, son:

   - reflexivas: R_7, R_{12}, R_{13} y R_{15};

- simétricas: R_0, R_1, R_4, R_7, R_8, R_{11}, R_{14} y R_{15};
- antisimétricas: R_0, R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_9, R_{10}, R_{12} y R_{13};
- transitivas: R_0, R_1, R_2, R_3, R_4, R_5, R_6, R_7, R_9, R_{10}, R_{12}, R_{13} y R_{15};
- conexas (fuertemente completas): R_{12}, R_{13} y R_{15}.

a. Son *de orden* (reflexivas, antisimétricas y transitivas): R_7, R_{12} y R_{13}.

b. Son *de orden total* (reflexivas, antisimétricas, transitivas y fuertemente completas): R_{12} y R_{13}.

c. Son *de equivalencia* (reflexivas, simétricas y transitivas): R_7 y R_{15}.

d. R_7 genera *dos clases de equivalencia*, $[0] = \{0\}$ y $[1] = \{1\}$; su conjunto cociente es

$$\{0,1\} \big/ R_7 = \{[0],[1]\} = \{\{0\},\{1\}\};$$

R_{15} genera *una única clase de equivalencia* $[0] = \{0,1\}$; su conjunto cociente es

$$\{0,1\} \big/ R_{15} = \{[0]\} = \{\{0,1\}\}.$$

■

Actividad 11.8

Sea $[\mathbb{N}]^{<\omega} = \{X \subset \mathbb{N} : X \text{ finito}\}$[29]. Supongamos que los elementos de los conjuntos pertenecientes a $[\mathbb{N}]^{<\omega}$ están siempre escritos en orden creciente, esto es, si $X \in [\mathbb{N}]^{<\omega}$ y $X = \{x_0, x_1, \ldots, x_k\}$ asumimos que $x_0 < x_1 < \cdots < x_k$. Sean $X, Y \in [\mathbb{N}]^{<\omega}$ e $I = \{0, 1, \ldots, \text{mín}(|X|, |Y|)\}$. Sea $X \wedge Y = \{x_0, x_1, \ldots, x_{p-1}\}$ si $x_0 = y_0, x_1 = y_1, \ldots, x_{p-1} = y_{p-1}$ y $x_p \neq y_p$. Demostremos que d_H y d_T, definidas por:

$$d_H(X,Y) = |\{i \in I : x_i \neq y_i\}| + \text{máx}(|X|,|Y|) - \text{mín}(|X|,|Y|), \quad \text{(métrica de Hamming)}$$
$$d_T(X,Y) = |X| + |Y| - 2|X \wedge Y|. \quad \text{(métrica del árbol)}$$

son métricas en $\mathbb{N}^k$.

§ 11.26.4 Cadena y anticadena

Definición 11.57.— Sean $(X; \preceq)$ un conjunto parcialmente ordenado y $Y \subseteq X$. Decimos que Y es una *cadena* precisamente si $(Y; \preceq)$ es un conjunto totalmente ordenado.

[29] ω es $\mathbb{N}$ considerado como ordinal, $< \omega$ indica finitud (*vid.* pág. 763 de esta edición).

Teorema 11.35
Si $(X; \preceq)$ es un conjunto totalmente ordenado e Y es un subconjunto no vacío de X, entonces $(Y; \preceq)$ es una cadena.

Ejemplo 349

Se satisface que:

0. $\forall n \in \mathbb{Z}^+, \left(\{n^k : k \in \mathbb{N}\}, |\right)$ es una cadena de $(\mathbb{N}; |)$;
1. cualquier subconjunto de números naturales con la relación de orden habitual es una cadena.

Definición 11.58.— Sean $(X; \preceq)$ un conjunto parcialmente ordenado y $Y \subseteq X$. Decimos que Y es una *anticadena* precisamente si todos sus elementos son incomparables, esto es, si, y sólo si, $\forall x, y \in Y, x \neq y \to x \npreceq y \wedge y \npreceq x$ (en otras palabras, si, y sólo si, $x \preceq y \to x = y$).

Ejemplo 350

Se satisface que:

0. en $\left(2^A \setminus \{\emptyset\}; \subseteq\right)$ dos conjuntos son incomparables si son disjuntos por lo que cualquier anticadena está formada por subconjuntos disjuntos de A;
1. cualquier subconjunto de naturales con la relación de igualdad es una anticadena.

§ 11.26.5 Cotas inferior y superior

Definición 11.59.— Sean $(X, \preceq)$ un conjunto ordenado, $x \in X$ e Y un subconjunto no vacío de X. Decimos que x es:

- *cota inferior* de Y en X precisamente si $(\forall y \in Y)(x \preceq y)$, esto es, si, y sólo si, x es anterior a todo elemento de Y;
- *cota superior* de Y en X precisamente si $(\forall y \in Y)(y \preceq x)$, esto es, si, y sólo si, x es posterior a todo elemento de Y.

Escribimos $\operatorname{cinf}(Y, X)$ para designar el conjunto de cotas inferiores de Y en X y $\operatorname{csup}(Y, X)$ para el conjunto de cotas superiores de Y en X.

Definición 11.60.— Sea $(X, \preceq)$ un conjunto ordenado e Y un subconjunto no vacío de X. Decimos que Y es:

- un *conjunto acotado inferiormente* en X precisamente si $\operatorname{cinf}(Y, X) \neq \emptyset$;

- un *conjunto acotado superiormente* en X precisamente si $\operatorname{csup}(Y, X) \neq \emptyset$;
- un *conjunto acotado* en X precisamente si es un conjunto acotado inferior y superiormente en X.

Definición 11.61.— Sean $(X, \preceq)$ un conjunto ordenado, $x \in X$ e Y un subconjunto no vacío de X. Decimos que x es:

- el *ínfimo* (o, sinónimamente, *extremo inferior*) de Y en X precisamente si $x \in \operatorname{cinf}(Y, X) \wedge (\forall y \in \operatorname{cinf}(Y, X))(y \preceq x)$, esto es, si, y sólo si, x es la mayor de las cotas inferiores de Y en X; notamos este hecho por $x = \operatorname{ínf}(Y, X)$;
- el *supremo* (o, sinónimamente, *extremo superior*) de Y en X, precisamente si $x \in \operatorname{csup}(Y, X) \wedge (\forall y \in \operatorname{csup}(Y, X))(x \preceq y)$, esto es, si, y sólo si, es la menor de las cotas superiores de Y en X; notamos este hecho por $x = \sup(Y, X)$.

Teorema 11.36 (Unicidad del ínfimo y del supremo)
El ínfimo y el supremo de un conjunto, si existen, son únicos.

Demostración.— En efecto, sean $(X, \preceq)$ un conjunto ordenado e Y un subconjunto no vacío de X; razonemos por reducción al absurdo para el ínfimo (para el supremo sería análogo): supongamos que existen $x, y \in X$, siendo $x \neq y$ y $x = \operatorname{ínf}(Y, X)$ e $y = \operatorname{ínf}(Y, X)$; de la definición de ínfimo se sigue que tanto x como y son cotas inferiores de Y en X; como $x = \operatorname{ínf}(Y, X)$, x es la mayor de las cotas inferiores, por lo que en particular, $y \preceq x$; y como como $y = \operatorname{ínf}(Y, X)$, y es la mayor de las cotas inferiores, por lo que en particular, $x \preceq y$; por tanto, por la antisimetría de $\preceq$, se tiene que $x = y$. ∎

Definición 11.62.— Sean $(X, \preceq)$ un conjunto ordenado, Y un subconjunto no vacío de X e $y \in Y$. Decimos que y es:

- *mínimo* (o, sinónimamente, *primer elemento*) de Y (en X) precisamente si $(\forall z \in Y)(y \preceq z)$, esto es, si, y sólo si, y es anterior a todos los elementos de Y; este hecho lo notamos $y = \operatorname{mín}(Y, X)$;
- *máximo* (o, sinónimamente, *último elemento*) de Y (en X) precisamente si $(\forall z \in Y)(z \preceq y)$, esto es, si, y sólo si, y es posterior a todos los elementos de Y; este hecho lo notamos por $y = \operatorname{máx}(Y, X)$.

Teorema 11.37 (Unicidad del mínimo y del máximo)
El mínimo y el máximo de un conjunto, si existen, son únicos.

Demostración.— En efecto, sean $(X, \preceq)$ un conjunto ordenado e Y un subconjunto no vacío de X; razonemos por reducción al absurdo para el mínimo (para el máximo sería análogo): supongamos que existen $x, y \in Y$, siendo $x \neq y$ y $x = \operatorname{mín}(Y, X)$ e $y = \operatorname{mín}(Y, X)$; por definición de mínimo,

como $x = \text{mín}(Y, X)$, x es menor o igual que todos los elementos de Y, en particular, $x \preceq y$ (ya que $y \in Y$, por ser el mínimo) y como $y = \text{mín}(Y, X)$, y es menor o igual que todos los elementos de Y, en particular $y \preceq x$ (ya que $x \in Y$, por ser el mínimo); por tanto, por la antisimetría de $\preceq$, $x = y$. ■

Definición 11.63.— Sean $(X, \preceq)$ un conjunto ordenado, Y un subconjunto no vacío de X e $y \in Y$. Decimos que y es:

- *minimal* de Y (en X) precisamente si $(\neg\exists z \in Y)(z \prec y)$, esto es, si, y sólo si, no existen elementos de Y anteriores estrictos a y;
- *maximal* de Y (en X) precisamente si $(\neg\exists z \in Y)(y \prec z)$, esto es, si, y sólo si, no existen elementos de Y posteriores estrictos a y.

Teorema 11.38

Si un elemento es mínimo (resp., máximo), entonces es minimal (resp., maximal).

Teorema 11.39

Si el orden es total, entonces mínimo (resp., máximo) y minimal (resp., maximal) son una misma cosa.

Ejemplo 351

Sea $A = \{1 + 1/n : n \in \mathbb{Z}^+\}$; es decir, $A = \{2, 1 + 1/2, 1 + 1/3, 1 + 1/4, \ldots\} \subset \mathbb{Q}$. Demostremos que $\text{csup}(A, \mathbb{Q}) = \{x \in \mathbb{Q} : 2 \leq x\}$.

Resolución.— En efecto, debido a la transitividad de $\leq$, bastará ver que todos los elementos de A son menores o iguales que el primer elemento de $\text{csup}(A, \mathbb{Q})$, esto es, si $(\forall x \in A)(x \leq 2)$. Debido a la forma de los elementos de A, esto equivale a si $(\forall n \in \mathbb{Z}^+)(1 \leq n)$, lo cual es cierto por definición de $\mathbb{Z}^+$.

También es sencillo demostrar que $\sup(A, \mathbb{Q}) = 2$, $\text{máx}(A, \mathbb{Q}) = 2$, $\text{cinf}(A, \mathbb{Q}) = \{x \in \mathbb{Q} : x \leq 1\}$, $\text{ínf}(A, \mathbb{Q}) = 1$ y que $\neg\exists\, \text{mín}(A, \mathbb{Q})$.

En relación a estos últimos, demostremos que $1 \notin A$. Por definición de A, $(\forall x \in A)(\exists n \in \mathbb{Z}^+)(x = 1 + 1/n)$, luego, preguntarnos si $1 \notin A$, equivale a preguntarnos si $(\forall n \in \mathbb{Z}^+)(1 + 1/n \neq 1)$, lo que es trivial, pues equivale a si $(\forall n \in \mathbb{Z}^+)(1/n \neq 0)$. ■

§ 11.26.6 Intervalos

Definición 11.64.— Sean $(X, \preceq)$ un conjunto ordenado e $I \subseteq X$. Decimos que I es un *intervalo* en X precisamente si $(\forall x, y \in I)(\forall z \in X)(x \preceq z \land z \preceq y \to z \in I)$.

Definición 11.65.— Dados un conjunto ordenado $(X, \preceq)$ y $x, y \in X$, con $x \preceq y$, distinguimos tres intervalos acotados de *extremos* x e y (también decimos de *origen* x y *extremo* y):

0. *abierto*: $\{z \in X : (x \prec z) \land (z \prec y)\}$, que notamos (x, y);
1. *cerrado*: $\{z \in X : (x \preceq z) \land (z \preceq y)\}$, que notamos $[x, y]$;
2. *semiabiertos* (o, sinónimamente, *semicerrados*): $\{z \in X : (x \preceq z) \land (z \prec y)\}$, que notamos $[x, y)$ y $\{z \in X : (x \prec z) \land (z \preceq y)\}$, que notamos $(x, y]$.

Observación 11.26.4.— Un procedimiento «teórico» para determinar si un conjunto es un intervalo pudiese ser el siguiente: X es un intervalo si, y sólo si, $(\forall x, y \in X)([x, y] \subseteq X)$.

§ 11.26.7 Segmento y sección

Definición 11.66.— Sean $(X, \preceq)$ un conjunto ordenado y $x \in X$. Llamamos *segmento determinado por* x al conjunto $S_x = \{y \in X : y \prec x\}$.

Ejemplo 352

En $(\mathbb{R}, \leq)$, el segmento determinado por $x \in \mathbb{R}$ es el intervalo $(\leftarrow, x)$.

Definición 11.67.— Sean $(X, \preceq)$ un conjunto ordenado, Y un subconjunto no vacío de X e $y \in Y$. Decimos que Y es una:

- *sección inicial abierta* de X de extremo y precisamente si $(\forall x \in X)(x \prec y \to x \in Y)$;
- *sección inicial cerrada* de X de extremo y precisamente si $(\forall x \in X)(x \preceq y \to x \in Y)$;
- *sección terminal* (o, sinónimamente, *sección final*) *abierta* de X de extremo y precisamente si $(\forall x \in X)(y \prec x \to x \in Y)$;
- *sección terminal* (o, sinónimamente, *sección final*) *cerrada* de X de extremo y precisamente si $(\forall x \in X)(y \preceq x \to x \in Y)$.

Observación 11.26.5.— Las definiciones de segmento y de sección inicial abierta quizás nos parezcan iguales. Pero sólo en apariencia[30].

[30] De hecho, en algunos textos aparecen las denominaciones de *segmento inicial* y *segmento terminal* como sinónimas de sección inicial y sección final, lo que contribuye a aumentar aún más la confusión.

Pensemos por ejemplo en $(\mathbb{Q}, \leq)$. Sucede ahí que todos los segmentos determinados por números racionales son secciones iniciales abiertas. Sin embargo, el recíproco no es cierto: la sección inicial abierta $Q^- \cup \{x \in : x^2 < 2\}$, es un segmento que no está determinado por un racional.

Definición 11.68.— Decimos que un conjunto ordenado $(X, \preceq)$ es un *conjunto ordenado completo* precisamente si toda sección inicial abierta está determinada por un elemento de X.

Ejemplo 353

0. $(\mathbb{Q}; \leq)$ no es un conjunto ordenado completo;
1. $(\mathbb{R}; \leq)$ sí es un conjunto ordenado completo.

§ 11.26.8 Orden bueno

Definición 11.69.— Decimos que un conjunto ordenado $(X, \preceq)$ está *bien ordenado* precisamente si todo subconjunto no vacío de X tiene mínimo.

Ejemplo 354

Siendo $\leq$ el orden habitual en los enteros, demostremos que:

0. $\left(\left\{3 + \frac{3}{n} : n \in \mathbb{Z}^+\right\}; \leq\right)$ no es un conjunto bien ordenado;
1. $(\mathbb{Z}; \leq)$ y $(\mathbb{Q}; \leq)$ no están bien ordenados;
2. $\mathbb{Z}$ está bien ordenado para otro orden;
3. $\mathbb{Q}$ está bien ordenado para otro orden.

Resolución.— En efecto:

0. sea $A = \left\{3 + \frac{3}{n} : n \in \mathbb{Z}^+\right\}$; A no está bien ordenado según el orden numérico habitual $\leq$, pues por ejemplo, $\neg\exists$ $\min(A, \mathbb{R})$ (de existir, sería 3, pero $3 \notin A$);
1. ni $\mathbb{Z}$ ni $\mathbb{Q}$ están bien ordenados según el orden numérico habitual $\leq$, pues por ejemplo, el conjunto de enteros pares no tiene mínimo;
2. $\mathbb{Z}$ sí está bien ordenado para el orden definido como sigue: $0 \prec -1 \prec 1 \prec -2 \prec 2 \prec \cdots \prec -n \prec n \prec \cdots$;[31]
3. tomaremos conciencia de ello cuando demostremos que $\mathbb{Q}$ es numerable.[32] ■

[31] *Vid. infra* observación 13.4.1 (pág. 730 de esta edición).
[32] *Vid. infra* § 13.4.1 (pág. 732 de esta edición).

Observación 11.26.6.— Notemos la diferencia con la *completitud fuerte de una relación*, la que pudiésemos expresar afirmando que todo subconjunto de dos elementos tiene mínimo.

Teorema 11.40
Si $(X, \preceq)$ está bien ordenado e Y es un subconjunto no vacío de X, entonces $(Y, \preceq)$ está bien ordenado.

Teorema 11.41
Todo conjunto bien ordenado está totalmente ordenado.

Demostración.— Sea X un conjunto bien ordenado por R. Sean $x, y \in X$. Como R es un orden bueno, x, y tiene elemento mínimo. Así, x es el mínimo o y es el mínimo. Pues bien, si x es el mínimo, entonces xRy, y si y es el mínimo, entonces yRx. Es decir, xRy o yRx; en definitiva, R es un orden total. ■

§ 11.26.9 Conjeturas

Destacamos dos:

- Conjetura $1/3 - 2/3$ (*cfr. v. gr.* https://en.wikipedia.org/wiki/1/3%E2%80%932/3_conjecture).
- Conjetura de la partición de oro (*cfr. v. gr.* https://en.wikipedia.org/wiki/1/3%E2%80%932/3_conjecture#Generalizations_and_related_results).

§ 11.27 Representación de una ordenación

§ 11.27.0 Reducciones reflexiva y transitiva de una relación

En sintonía con las reducciones reflexiva y transitiva de un grafo[33], tenemos las correspondientes de una relación.

Definición 11.70.— Llamamos *reducción reflexiva de una relación* diádica R en X a la menor relación en X, en el sentido de $\subseteq$, con la misma clausura reflexiva[34] que R; justamente es $R \setminus I_X$.

Definición 11.71.— Llamamos *reducción transitiva de una relación* diádica R en X a la menor relación en X, en el sentido de $\subseteq$, con la misma clausura transitiva[34] que R.

[33] *Cfr. infra* § 8.6 (pág. xci de esta edición).
[34] *Cfr. supra* § 11.25 (pág. 641 de esta edición).

§ 11.27.1 Diagrama de Hasse

Definición 11.72.— Un *diagrama de* Hasse de un preorden parcial (esto es, una relación reflexiva y transitiva), es el grafo que queda tras hacer en el digrafo de la relación lo siguiente:

0. le aplicamos una reducción reflexiva (esto es, damos por implícita la reflexiva en el diagrama y no dibujamos los lazos)[33];
1. le aplicamos una reducción transitiva (es decir, damos por implícita la transitiva en el diagrama y no dibujamos las aristas correspondiente a la conclusiones por transitividad)[33], y
2. la orientación de cada arista también la damos por implícita y viene dada por el posicionamiento del nodo inicial de la arista en una posición inferior del nodo terminal, es decir, las aristas están orientadas de abajo arriba.

Ejemplo 355 (Diagrama de Hasse del álgebra de Boole B_n)

Convenimos en que B_n designa el álgebra de Boole del conjunto de subconjuntos de $\{0, 1, \ldots, n\}$ ordenado por la inclusión de conjuntos ($Y \preceq X$ significa $Y \subseteq X$).

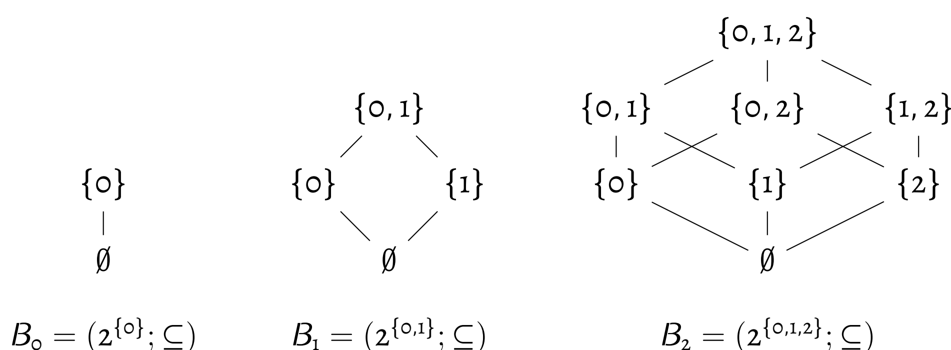


Figura 11.7.— Diagramas de Hasse de B_0, B_1 y B_2.

[Cubit 80].

Ejemplo 356 (Diagrama de Hasse de los divisores positivos D_n)

Convenimos en que D_n designa el conjunto de todos los divisores positivos de n; pensemos en D_{12}, es decir, en $\{1, 2, 3, 4, 6, 12\}$, y en estar éste ordenado por la relación de divisibilidad en $\mathbb{Z}^+$ ($y \preceq x$ significa $y|x$, estando ésta en $\mathbb{Z}^+$ definida $\forall x, y \in \mathbb{Z}^+$ por $y|x$ si, y sólo si, $(\exists z \in \mathbb{Z}^+)(y \cdot z = x)$.

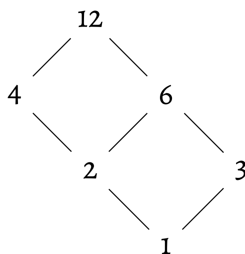


Figura 11.8.— Diagrama de Hasse de $(D_{12}; \mid)$.

Observación 11.27.0.— Pudiésemos utilizar el artefacto en línea SageMath[35] y el siguiente programita en lenguaje Sage para dibujar el diagrama de Hasse de $(D_{60}; \mid)$, con dos abordajes, manual y automático,

[Cubit 81].

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
# (doc: https://doc.sagemath.org/html/en/reference/combinat/sage/combinat/posets/posets.html)

## # Manual
D60 = Poset({ 1:[2,3,5], 2:[4,6,10], 3:[6,15], 4:[12,20], 5:[10,15], 6:[12,30], 10:[20,30],
        12:[60], 15:[30], 20:[60], 30:[60] })
D60.show()
# devuelve: <el diagrama de Hasse de (D60,|)>

## # Automático
D60 = Poset((divisors(60), attrcall("divides"))) # ordenados por subconjuntos de múltiplos
D60 = Poset((divisors(60), attrcall("divides")), linear_extension=True) # en orden creciente
D60.list()
# devuelve: [1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60]
D60.cover_relations()
# devuelve: [[1, 2], [1, 3], [1, 5], [2, 4], [2, 6], [2, 10], [3, 6], [3, 15], [4, 12], [4, 20],
# [5, 10], [5, 15], [6, 12], [6, 30], [10, 20], [10, 30], [12, 60], [15, 30], [20, 60], [30, 60]]
D60.show()
# devuelve: <el diagrama de Hasse de (D60,|)>
```

que devuelve duplicada (generación manual y automática) la imagen visualizada en la figura 11.9 (pág. 661 de esta edición).

[35] *Cfr. supra* § 11 (pág. cii de esta edición).

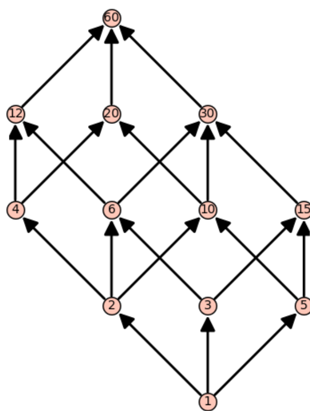


Figura 11.9.— Diagrama de Hasse de $(D_{60}; |)$. Resultado de la ejecución del programa anterior en SageMathCell. Observemos la particularidad de la representación por defecto con arcos (aristas dirigidas).

Actividad 11.9

Sea Π_n el conjunto de todas las particiones del conjunto $\{0, 1, \ldots, n\}$ y pensemos en ordenar dicho conjunto por refinamiento, esto es, dadas dos particiones, σ y τ, $\sigma \preceq \tau$ significa que todo $\sigma_i \in \sigma$ es subconjunto de algún $\tau_{j(i)} \in \tau$. Representemos los diagramas de Hasse de $(\Pi_0; \preceq)$, $(\Pi_1; \preceq)$ y $(\Pi_2; \preceq)$.

§ 11.28 Muestra de más ejemplos

Ejemplo 357

Sean el alfabeto $\Sigma = \{0, 1\}$, C el conjunto de todas las palabras (palabras binarias finitas, incluida la palabra vacía) y $+$ la operación diádica de concatenación en C (a modo de ilustración, si $x = 010$, $y = 10$ y $z = 01$, entonces, por ejemplo, $x + y + z = 0101001$ y $z + x + y = 0101010$). Sea Σ^* el monoide abeliano $(C; +)$ (la palabra vacía ϵ es el neutro). Sea $\preccurlyeq$ la relación diádica definida en Σ^* por:

$$(\forall s_1, s_2 \in \Sigma^*)\,(s_1 \preccurlyeq s_2 \leftrightarrow (\exists c, c' \in \Sigma^*)(s_2 = c + s_1 + c'))\,.$$

0. Demostremos si $\preccurlyeq$ satisface o no las propiedades: I, reflexiva; II, simétrica; III, antisimétrica; IV, transitiva, y V, conexa, y digamos: VI, qué tipo de relación es, y VII, por qué;
1. Proporcionemos un ejemplo de conjunto C y considerando actuando en $\Sigma^* = (C; +)$, mostremos cuáles son las clases de equivalencia, las clases de tolerancia o dibujemos un diagrama de Hasse, dependiendo de que $\preccurlyeq$ sea una relación de equivalencia, una relación de tolerancia o una relación de orden en Σ^*.

[EFE 25.6.2019:2a].

Resolución.—

0. Dadas cualesquiera palabras binarias s_1 y s_2 de Σ^*, entonces:

   I. $\preccurlyeq$ es reflexiva, pues para cualquier $s \in C$, $\epsilon + s + \epsilon = s$;

   II. $\preccurlyeq$ no es simétrica, pues, por ejemplo, $1 \preccurlyeq 010$ ($c = c' = 0$), pero no existen d y d' en Σ^* tales que $1 = d + 010 + d'$, por lo que $010 \not\preccurlyeq 1$;

   III. $\preccurlyeq$ es antisimétrica; en efecto, $\forall s_1, s_2 \in \Sigma^*$:

$$s_1 \preccurlyeq s_2 \leftrightarrow (\exists c, c' \in \Sigma^*)(s_2 = c + s_1 + c'), \tag{11.11}$$
$$s_2 \preccurlyeq s_1 \leftrightarrow (\exists d, d' \in \Sigma^*)(s_1 = d + s_2 + d'), \tag{11.12}$$

de donde:

$$\begin{aligned} s_1 &= d + s_2 + d' && \text{(por (11.12))}\\ &= d + (c + s_1 + c') + d' && \text{(por (11.11))}\\ &= (d + c) + s_1 + (c' + d'), && \text{(+ es asociativa)} \end{aligned}$$

de donde necesariamente por definición de concatenación de palabras, $d+c = \epsilon$ y $c'+d' = \epsilon$, por lo que $c = c' = d = d' = \epsilon$ y por tanto, $s_1 = s_2$;

IV. $\preccurlyeq$ es transitiva; así es, $\forall s_1, s_2, s_3 \in \Sigma^*$:

$$s_1 \preccurlyeq s_2 \leftrightarrow (\exists c, c' \in \Sigma^*)(s_2 = c + s_1 + c'), \tag{11.13}$$

$$s_2 \preccurlyeq s_3 \leftrightarrow (\exists d, d' \in \Sigma^*)(s_3 = d + s_2 + d'), \tag{11.14}$$

de donde:

$$\begin{aligned} s_3 &= d + s_2 + d' && \text{(por (11.14))} \\ &= d + (c + s_1 + c') + d' && \text{(por (11.13))} \\ &= (d + c) + s_1 + (c' + d') && \text{(+ es asociativa)} \\ &= f + s_1 + f', && \text{(+ es operación)} \end{aligned}$$

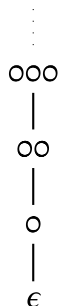
con $f, f' \in \Sigma^*$ (ya que $f = d + c$ y $f' = c' + d'$ y $+$ es operación en Σ^*), y por tanto, $s_1 \preccurlyeq s_3$;

V. sin embargo, $\preccurlyeq$ no es conexa (fuertemente completa), ya que, por ejemplo, las palabras 0 y 1 no son comparables por $\preccurlyeq$ (por un lado, $0 \not\preccurlyeq 1$ ya que no existen c y c' en Σ^* tales que $1 = c + 0 + c'$; por otro, $1 \not\preccurlyeq 0$ pues tampoco existen c y c' en Σ^* tales que $0 = c + 1 + c'$);

VI. $\preccurlyeq$ es una relación de orden parcial;

VII. $\preccurlyeq$ es una relación de orden parcial porque satisface las propiedades reflexiva, antisimétrica y transitiva (y no es total porque no satisface la conexa).

1. Sea, por ejemplo, $\Sigma = \{0\}$, $C = \{\epsilon, 0, 00, 000, \ldots\}$ y $\Sigma^* = (C; +)$. El diagrama de Hasse de $\preccurlyeq$, en este caso un orden total en Σ^*, puede dibujarse sólo parcialmente, por ser infinito numerable el número total de palabras (su cardinal es el mismo que el de $\mathbb{N}$):





§ 11.29 Relación de preferencia

§ 11.29.0 Toma de decisiones

Nos sumergimos en el ámbito de la *toma de decisiones*. Mencionar primero que según varios estudios —*cfr. v. gr.* Chipman [171]; White [172] (pág. 31); Jansana [160] (pág. 60); Ríos Insúa, Bielza Lozoya y Mateos Caballero [161] (pág. 31); Escribano [173] (pág. 47)— de las propiedades estudiadas en la definición 11.31 (pág. 615 de esta edición) —y posteriormente en la definición 2.0.3 (pág. 183 de esta edición) y en la definición 2.0.3 (pág. 183 de esta edición), las más frecuentes sobre todo en cuanto al uso de las relaciones de orden en las teorías de la elección, el valor y la incertidumbre, tan esenciales para la buena desenvoltura son las que recogemos en el cuadro 11.2.

Propiedades de una relación diádica		
Reflexiva	(R)	$(\forall a \in C)(aRa)$
Irreflexiva	(I)	$(\forall a \in C)(a\neg Ra)$
Simétrica	(S)	$(\forall a, b \in C)(aRb \to bRa)$
Asimétrica	(A)	$(\forall a, b \in C)(aRb \to b\neg Ra)$
Antisimétrica	(An)	$(\forall a, b \in C)(aRb \wedge bRa \to a \approx b)$
Transitiva	(T)	$(\forall a, b, c \in C)(aRb \wedge bRc \to aRc)$
Idempotencia	(Id)	$(\forall a, b, c \in C)(aRb \wedge bRc \leftrightarrow aRc)$
Negativamente transitiva	(nT)	$(\forall a, b, c \in C)(a\neg Rb \wedge b\neg Rc \to a\neg Rc)$
Serial	(Se)	$(\forall a \in C)(\exists b \in C)(aRb)$
Dirección	(Di)	$(\forall a, b \in C)(\exists c \in C)(cRa \wedge cRb)$
Contradirección	(Cdi)	$(\forall a, b \in C)(\exists c \in C)(aRc \wedge bRc)$
Euclidea	(E)	$(\forall a, b, c \in C)(aRb \wedge aRc \to bRc)$
Proyección	(F)	$(\forall a, b, c \in C)(aRb \wedge aRc \to b \approx c)$
Proyección C^C	(Fc)	$(\forall a \in C)(\exists! b \in C)(aRb)$
Asignación	(As)	$(\forall a, b, c \in C)(bRa \wedge cRa \to b \approx c)$
Débilmente densa	(D)	$(\forall a, b \in C)(aRb \to (\exists c \in C)(aRc \wedge cRb))$
Débilmente dirigida	(Dd)	$(\forall a, b, c \in C)(aRb \wedge aRc \to (\exists d \in C)(bRd \wedge cRd))$
Completitud débil	(Cd)	$(\forall a, b, c \in C)(aRb \wedge aRc \to bRc \vee cRb \vee b \approx c)$
Completitud	(C)	$(\forall a, b \in C)(a \not\approx b \to aRb \vee bRa)$
Completitud fuerte	(Cf)	$(\forall a, b \in C)(aRb \vee bRa)$
Relación de Ferrers	(Fe)	$(\forall a, b, c, d \in C)(aRb \wedge cRd \to aRd \vee cRb)$
Semi-transitiva	(St)	$(\forall a, b, c \in C)(aRb \wedge bRc \to (\exists d \in C)(aRd \vee dRc))$
Trivialidad	(Tr)	$(\forall a, b \in C)(aRb)$
Vacuidad	(V)	$(\forall a, b \in C)(a\neg Rb)$

Cuadro 11.2.— Propiedades frecuentemente satisfechas por una relación diádica R definida sobre un conjunto no vacío C.

Suponemos que disponemos de varias *alternativas* —o *cursos de acción*— conducentes cada una a un fin determinado, a una *consecuencia*, a un *efecto* o *resultado*.

Actuaremos teniendo presentes varios *principios*:

- *principio de consistencia*: debemos exluir del proceso toda proposición insatisfactible;

Según sea nuestro conocimiento del *ambiente* —*estado de la naturaleza* o *contexto*— del proceso de toma de decisiones, éste es:

- de *certidumbre*, si para toda alternativa y estado de la naturaleza conocemos la consecuencia de elegirla;
- de *riesgo*, si no conocemos las consecuencias pero nos es posible asignarles una distribución de probabilidad según la elección de la alternativa y el estado de la naturaleza;
- de *incertidumbre*, si no estamos en ninguno de los contextos anteriores, es decir, cuando no conocemos los estados de la naturaleza ni las consecuencias ni disponemos de información empírica ni objetiva que nos permita una asignación de probabilidades o creencias;
- de *conflicto*, si conocemos que los estados de la naturaleza están controlados por antagonistas, contendientes u oponentes —problema usualmente abordado desde la *teoría de juegos*—.

Sea cual sea el ambiente, el proceso de toma de decisiones consta de cinco *fases esenciales*:

0. *definición de la situación de decisión* concreta en análisis, recurriendo usualmente a la comparación con situaciones pasadas —memoria—;
1. *identificación de los estados de la naturaleza y de las alternativas —cursos de acción—* que se le presentan a quien decide en dicha situación concreta;
2. *predicción de las consecuencias* de la elección de cada alternativa, habitualmente por inferencia inductiva a partir de un conjunto de datos;
3. *valoración de las consecuencias* resultantes usando *escalas*, cualitativas o cuantitativas, representativas del grado de *admisibilidad* e incluso *deseabilidad* de estas consecuencias por parte de quien decide;
4. *elección de la alternativa*, del curso de acción, mediante un criterio de decisión previamente elegido.

Surge así el concepto de *preferencia* entre alternativas —tener en más una alternativa a otra— y el de su dual, la *postergación* —tener en menos una alternativa a otra—.

Ejemplo 358

Para la realización de una tarea en la que tenemos gran experiencia —que en cualquier caso nos llevará 1 hora y cuyo valor estimamos en 20 unidades monetarias (u.m.)—, tenemos la posibilidad de no ofrecer nuestro tiempo o de ofrecerlo, en cuyo caso resulta viable hacerlo de tres formas distintas: cobrando, trocándolo o regalándolo. Estimamos que nuestro tiempo puede ser demandado por cinco personas como mucho —es decir, hemos reservado cinco horas de nuestro tiempo futuro—. Dentro de lo difícil que es transformar lo cualitativo en cuantitativo, hacemos una asignación a nuestro grado de satisfacción personal —beneficio— que recibiríamos por cada curso de acción: $s_1 = 30$ —vendemos la hora de nuestro tiempo para esa tarea en 30 u.m.—, $s_2 = 40$ —valoramos la satisfacción del trueque en 40 u.m.— y $s_3 = 70$ —valoramos en 70 u.m. la satisfacción de regalar nuestro tiempo—. Se trata de que averigüemos cuál es la mejor alternativa.

Resolución.— El estado de la naturaleza corresponde a la demanda de nuestro tiempo. Identificamos seis estados de la naturaleza que designamos por:

E_0 0 horas, nadie lo demanda;
E_1 1 hora, una persona lo demanda;
⋮
E_5 5 horas, cinco personas lo demandan.

Asimismo, identificamos cuatro alternativas:

A_0 no ofrecemos nuestro tiempo;
A_1 vendemos nuestro tiempo;
A_2 trocamos nuestro tiempo;
A_3 regalamos nuestro tiempo.

Si hemos ofrecido nuestro tiempo, hemos estimado en 20 u.m. la hora y hemos reservado 5 horas de nuestro tiempo, entonces, cuantitativamente, es como si hubiésemos hecho una «inversión/-desembolso» inicial de $20 \times 5 = 100$ u.m. Por otro lado, el «ingreso» correspondiente al estado E_j es $s_i \times j$. Notemos que en esta perspectiva utilitarista que protagoniza el contexto de certidumbre, la satisfacción personal es el beneficio, siendo éste el ingreso menos el desembolso.

Para cada alternativa, la obtención de las valoraciones de las consecuencias responde a una ecuación —llamada usualmente *función de resultados* (o *de pagos*)— que en este caso es la de una recta, $s_i \times j + d$, siendo $d = -100$ y siendo s_i los anteriores y j el índice identificador del estado de la naturaleza. Así, por ejemplo, para A_2 y E_3 es $s_2 \times 3 + (-100) = 40 \times 3 - 100 = 20$ u.m.

Si no ofrecemos nuestro tiempo tanto la inversión inicial como el beneficio han sido nulos —primera línea del cuadro, correspondiente a la alternativa A_0—.

	E_0	E_1	E_2	E_3	E_4	E_5
A_0	0	0	0	0	0	0
A_1	−100	−70	−40	−10	20	50
A_2	−100	−60	−20	20	60	100
A_3	−100	−30	40	110	180	250

Para los estados E_0 y E_1, esto es, si estimamos que como mucho una persona se va a interesar por nuestro tiempo, la alternativa preferible es la A_0, no ofrecerlo. Sin embargo, con la valoración cuantitativa que hemos heho, desde el momento que consideremos que al menos dos personas se interesarán por nuestro tiempo, la alternativa preferible es la A_3, regalarlo. ■

§ 11.29.1 Ordenaciones de preferencia en ambiente de certidumbre

En este primer acercamiento que hacemos en estas notas supondremos que trabajamos en un *ambiente de certidumbre*, esto es, que para toda alternativa se conoce su consecuencia. Llamemos Ω al *conjunto de consecuencias*[36] $x, y, z, x_0, x_1, \ldots$.

Definimos en Ω una relación diádica $\succsim$ —*relación de preferencia*— tal que dados dos elementos x e y de Ω algunas lecturas posibles de $x \succsim y$ sean:

- «quien decide prefiere x a y o le son indiferentes»,
- «x es al menos tan preferido como y»,
- «y es como mucho tan preferido como x»,
- «y no es preferido a x».

Consideramos también su dual $\precsim$ —*relación de postergación*— con sus correspondientes lecturas de $x \precsim y$ para cualesquiera x e y de Ω:

- «quien decide posterga x a y o le son indiferentes» —«quien decide prefiere y a x o le son indiferentes»—,
- «x es al menos tan postergado como x» —«y es al menos tan preferido como x»—,
- «y es como mucho tan postergado como x» —«x es como mucho tan preferido como y»—,
- «y no es postergado a x» —«x no es preferido a y»—.

[36] En el ambiente de certidumbre en el que hacemos la exposición, da igual interpretar Ω como el conjunto de alternativas o consecuencias.

La lectura de la ocurrencia simultánea de $x \succsim y$ y de $y \succsim x$ —o de $x \precsim y$ y de $y \precsim x$— es la indiferencia entre x e y:

- «x e y son indiferentes»,
- «x e y son igualmente deseables para quien decide»,

que notamos $x \sim y$, expresión de una nueva relación diádica $\sim$ —*relación de indiferencia*— en Ω.

Si $x \succsim y$ y no $x \sim y$, decimos que «x es preferido a y», cosa que designamos por $x \succ y$, expresión de una nueva relación diádica $\succ$ en Ω. De manera similar, si $x \precsim y$ y no $x \sim y$ decimos que «x es menos preferido que y» y notamos por $x \prec y$, expresión de una nueva relación diádica $\prec$ en Ω.

Diremos que

- $\succ$ es una *relación de preferencia estricta* —también llamada *relación de orden débil estricto*—,
- $\sim$ es una *relación de indiferencia*, y
- $\succsim$ es una *relación de preferencia débil* —o de preferencia-indiferencia—.

Las duales de $\succ$ y $\succsim$ son, respectivamente

- $\prec$, una *relación de postergación estricta*, y
- $\precsim$, una *relación de postergación débil* —o de postergación-indiferencia—.

Sólo a modo de ejemplo, mostramos dos caminos para definir estas relaciones en el sentido de la preferencia.

0.º) Pudiésemos comenzar definiendo una relación de preferencia estricta $\succ$ en Ω como aquélla que satisface:

I. $(\forall x, y \in \Omega)(x \succ y \rightarrow y \not\succ x)$; ($\succ$ es asimétrica en Ω)

II. $(\forall x, y, z \in \Omega)(x \not\succ y \wedge y \not\succ z \rightarrow x \not\succ z)$. ($\succ$ es negativamente transitiva en Ω)

Observemos que de aquí, $\succ$ es irreflexiva, antisimétrica y transitiva, en otras palabras, $\succ$ es un orden parcial estricto antisimétrico.

A continuación, pudiésemos relajar la condición de ser estricta en ambos sentidos. Esto es para permitir la *indiferencia* en la decisión, es decir, una relación que satisface, $\forall x, y \in \Omega$,

$$x \sim y \leftrightarrow (x \not\succ y) \wedge (y \not\succ x), \tag{11.15}$$

o implícitamente,

$$x \succ y \leftrightarrow (y \not\succ x) \wedge (y \nsim x),$$

pudiendo, en cualquier caso, definir ahora una *relación de preferencia débil* en Ω, $\forall x, y \in \Omega$,

$$x \succsim y \leftrightarrow (x \succ y) \vee (x \sim y). \tag{11.16}$$

Entonces, pudiésemos demostrar que $\forall x, y \in \Omega$,

0. $\succ$ es asimétrica si, y sólo si, $\succsim$ es fuertemente completa;

1. $\succ$ es negativamente transitiva si, y sólo si, $\succsim$ es transitiva.

Observemos que como ser fuertemente completa implica ser reflexiva —y completa—, tenemos que $\succsim$ es reflexiva, transitiva y fuertemente completa, en otras palabras, $\succsim$ es una relación de preorden.

En resumen, a partir de la relación de preferencia estricta $\succ$ hemos definido la indiferencia $\sim$ y, con ambas, la relación de preferencia débil $\succsim$, consiguiendo que todos los elementos sean comparables con esta última.

Por otro lado, la relación de indiferencia $\sim$ es una relación de equivalencia:

- $\sim$ es reflexiva: $(\forall x)(x \sim x \leftrightarrow x \not\succ x)$, esto es, $\sim$ es reflexiva si, y sólo si, $\succ$ es irreflexiva (que lo es);
- $\sim$ es simétrica: $(\forall x, y)(x \sim y \leftrightarrow (x \not\succ y) \wedge (y \not\succ x) \leftrightarrow (y \not\succ x) \wedge (x \not\succ y) \leftrightarrow y \sim x)$;
- $\sim$ es transitiva: $(\forall x, y, z)((x \sim y) \wedge (y \sim z) \leftrightarrow ((x \not\succ y) \wedge (y \not\succ x)) \wedge ((y \not\succ z) \wedge (z \not\succ y)) \rightarrow ((x \not\succ z) \wedge (z \not\succ x))$ [por ser $\succ$ negativamente transitiva] $\leftrightarrow x \sim z$ [por definición de $\sim$]).

1.°) Otro camino es considerar como concepto primitivo un *preorden parcial de preferencia* $\succsim$, esto es una relación diádica en Ω, reflexiva y transitiva[37] y definir la *indiferencia* en Ω, $\forall x, y \in \Omega$,

$$x \sim y \leftrightarrow (x \succsim y) \wedge (y \succsim x), \tag{11.17}$$

El hecho de que en ambos caminos la relación de indiferencia $\sim$ sea una relación de equivalencia, nos permite en cualquiera de ellos clasificar las consecuencias. Como es lo habitual en las relaciones de equivalencia, consideraríamos el conjunto cociente $\Omega/\sim$ y clasificaríamos los resultados en clases de equivalencia, llamadas aquí *clases de consecuencias indiferentes*.

Las decisiones —meditadas— que tomamos en nuestros *actos de elección* son decisiones de orden basadas en medidas generales o específicas. Pudiésemos elegir una entidad entre varias, todas serían comparables —bastaría partir de un preorden o de un orden total de preferencia— y todas estarían

[37] En vez de un preorden de preferencia pudiésemos considerar que también satisficiese la antisimétrica (*orden parcial de preferencia*), la compleción fuerte (*preorden de preferencia*) o ambas (*orden total de preferencia*).

clasificadas y ordenadas de acuerdo a nuestras preferencias —diríamos que habríamos conseguido definir una *estructura de preferencias* en la colección de entidades—.

Ejemplo 359

Demostremos que el juego Piedra, papel o tijeras posee una *estructura de preferencias no transitiva*, esto es, viene definida por una relación reflexiva y no transitiva.

Resolución.— En efecto, es reflexiva —cada alternativa es preferida a sí misma, de ahí los empates piedra–piedra, papel–papel y tijeras–tijeras— y es circular —la piedra es preferida a las tijeras, las tijeras son preferidas al papel, pero el papel es preferido a la piedra— y, por tanto, no transitiva —ninguna alternativa es la más preferida, pues, en número, son las mismas las opciones de ganar que de perder—.

Por otro lado, observemos, sólo a modo de ejemplo, que sí es asimétrica —si se da una preferencia nunca se da la recíproca— y antisimétrica —pues los únicos casos de indiferencia se producen cuando las alternativas son la misma—, si bien no es negativamente transitiva —ya que aunque la piedra no es preferida al papel y el papel no es preferido a las tijeras, la piedra sí es preferida a las tijeras—. ■

Observación 11.29.0.— Pudiese interesar conocer que del juego Piedra, papel o tijeras, existen competiciones donde enfrentar estrategias y sus correspondientes algoritmos[38].

§ 11.30 En relación con la algoritmia

Dada una sucesión y una relación de orden aplicable a cualesquiera dos términos de dicha sucesión, se trata de disponer todos los términos de esta última en una nueva sucesión de acuerdo a dicha relación de orden. Distinguimos entre:

- los *algoritmos de ordenación*[39], que presuponen la no existencia de ningún orden previo (preordenación) en la sucesión de partida, y
- los *algoritmos de ordenación adaptativa*[40] que tratan de descubrir subsucesiones ordenadas según la relación —o según otra conocida— y de aprovechar la existencia de dichas preordenaciones para acelerar así la ordenación de la sucesión original.

[38] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Rock_paper_scissors#Algorithms.
[39] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Algoritmo_de_ordenamiento.
[40] *Cfr. v. gr.* https://pt.wikipedia.org/wiki/Ordenação_adaptativa.

Ejemplo 360

> ¿Es el recuento del número de inversiones una buena *medida de preordenación* o *medida de desorden*?

Resolución.— No, por ejemplo, imaginemos que quisiéramos ordenar según la relación $\leq$ la sucesión finita $\langle 5, 6, 7, 8, 9, 0, 1, 2, 3, 4 \rangle$, ésta tiene 25 inversiones por lo que pudiésemos pensar que está muy desordenada, sin embargo se trata de una sucesión casi ordenada según $\leq$ con dos preordenaciones claras, dos subcesiones finitas crecientes, las subsucesiones finitas $\langle 5, 6, 7, 8, 9 \rangle$ y $\langle 0, 1, 2, 3, 4 \rangle$ y sólo haría falta mover la segunda delante de la primera para conseguir ordenar la sucesión original de la manera pretendida —en otras palabras, si considerásemos movimientos de subconjuntos de términos y no sólo de éstos y redefiniésemos el concepto de inversión, el número de éstas se reduciría a 1—. ■

Observación 11.30.0.— En cuanto a medida de preordenación y medida de desorden, *cfr. v. gr.* Estivill-Castro y Wood, [174] y [175], respectivamente. Respecto al recuento de inversiones, *vid. v. gr.* Count Inversions in an array | Set 1 (Using Merge Sort), *GeeksforGeeks* (https://www.geeksforgeeks.org/counting-inversions/).

No olvidemos los algoritmos de búsqueda en una sucesión finita, por ejemplo, la *búsqueda lineal* (o, sinónimamente, *búsqueda secuencial*) (cuando la sucesión conforma un conjunto o un conjunto totalmente ordenado)[41] y la *búsqueda binaria* (o, sinónimamente, *búsqueda de intervalo medio*, *búsqueda logarítmica* o *búsqueda de corte binario*) (cuando la sucesión conforma un conjunto totalmente ordenado)[42].

Destacables son también los algoritmos de recorrido de árboles y grafos, por ejemplo, la *búsqueda en anchura*[43] —*Breadth First Search* (BFS)— (que utilizamos para nombrar los nodos de un árbol semántico en el algoritmo TA/S) y la *búsqueda en profundidad*[44] —*Depth First Search* (DFS)—.

§ 11.31 Propuesta de más actividades

Es recomendable que *para cada relación* que aparezca en esta selección, *determinemos su inversa* y *representemos ambas* mediante *diagramas de coordenadas*, *matrices*, *correspondencias*, *grafos dirigidos o no dirigidos*, *diagramas de vecindad* (en el caso de relaciones de tolerancia) y pensemos de ambas (de la relación y su inversa) si son funciones o no.

[41] *Vid. v. gr.* https://es.wikipedia.org/wiki/Búsqueda_lineal.
[42] *Vid. v. gr.* https://en.wikipedia.org/wiki/Binary_search_algorithm.
[43] *Vid. v. gr.* https://en.wikipedia.org/wiki/Breadth-first_search.
[44] *Vid. v. gr.* https://en.wikipedia.org/wiki/Depth-first_search.

En el caso de ordenaciones, dibujemos un diagrama simplificado que sólo muestre las conexiones entre los predecesores o sucesores directos (*diagrama de* HASSE). Reflexionemos sobre la *identificación algorítmica de propiedades a partir de las distintas representaciones de una relación*.

Actividad 11.10

Sean X e Y dos conjuntos cualesquiera. ¿Es $\{X \setminus Y, X \cap Y, Y \setminus X\}$ una partición de X?

Actividad 11.11

Sean X e Y dos conjuntos cualesquiera. Demostremos que $\{X \setminus Y, X \cap Y, Y \setminus X, X^{\complement} \cap Y^{\complement}\}$ es una partición del universal.

[Cubit 67].

Con miras a su resolución.— Utilicemos el artefacto en línea Symbolab[45] como apoyo, si bien nos queda el trabajo de anotar con las propiedades aplicadas las demostraciones que nos ofrece. Comprobemos las tres exigencias para ser partición:

- que son subconjuntos del universal es trivial;
- que son subconjuntos disjuntos dos a dos, esto es, que sus intersecciones dos a dos son el conjunto vacío, con las entradas

```
(A \cap B^c) \cap (A \cap B)
(A \cap B^c) \cap (A^c \cap B)
(A \cap B^c) \cap (A^c \cap B^c)
(A \cap B) \cap (A^c \cap B)
(A \cap B) \cap (A^c \cap B^c)
(A^c \cap B) \cap (A^c \cap B^c)
```

- que la unión es el universal con la entrada

```
(A \cap B^c) \cup (A \cap B) \cup (A^c \cap B) \cup (A^c \cap B^c)
```

Actividad 11.12

Sean $X = \{x \in \mathbb{Z} : x \geq 0\}$ e $Y = \{x \in \mathbb{Z} : x < 0\}$. Demostremos que $\{X, Y\}$ es una partición de $\mathbb{Z}$.

Actividad 11.13

¿Es toda relación diádica una aplicación? ¿Es toda aplicación una relación diádica?

[45] *Vid.* https://es.symbolab.com/solver/step-by-step/.

Actividad 11.14

Sea R una relación diádica definida en un conjunto X, no vacío, simétrica y transitiva en X y tal que $(\forall x \in X)(\exists y \in X)(xRy)$. ¿Es R reflexiva en X?

Actividad 11.15

Proporcionemos ejemplos de relaciones que sean: 0., irreflexiva y reflexiva; 1., irreflexiva y no reflexiva; 2., no irreflexiva y reflexiva, y 3., ni irreflexiva ni reflexiva.

[Cubit 82].

Actividad 11.16

Sea la relación diádica R en $\mathbb{N}$ definida por $(\forall m, n \in \mathbb{N})(mRn \leftrightarrow m^2 = n^2)$. Estudiémosla.

Actividad 11.17

Demostremos que la relación R en $\mathbb{R}$ definida por $(\forall x, y \in \mathbb{R})(xRy \leftrightarrow x^3 - y^3 = x - y)$ es una relación de equivalencia en $\mathbb{R}$.

Actividad 11.18

Sea O un punto fijo en el conjunto P de todos los puntos del plano euclideo, sean A y B dos puntos arbitrarios de P.

0. Sea la relación diádica $A\,R\,B$ si, y sólo si, longitud euclidea de OA = longitud euclidea de OB —la distancia euclidea en el plano es $d_2((x_0, y_0), (x_1, y_1)) = (|x_0 - x_1|^2 + |y_0 - y_1|^2)^{1/2}$—.
   a. Demostremos que R es una relación de equivalencia en P.
   b. Hallemos las clases de equivalencia y el conjunto cociente.
1. ¿Qué forma tienen las clases de equivalencia si en vez de medir con la distancia euclidea medimos con la distancia de Manhattan*, $d_1((x_0, y_0), (x_1, y_1)) = |x_0 - x_1| + |y_0 - y_1|$?, ¿y si medimos con la distancia de CHEBYCHEV, $d_\infty = \text{máx}\{|x_0 - x_1|, |y_0 - y_1|\}$?

[Cubit 70].

---

* *Cfr. v. gr.* Eugene F. KRAUSE, *Taxicab Geometry*, Dover, 1986.

Actividad 11.19

Hagamos lo siguiente.

0. Demostremos que toda relación de equivalencia en un conjunto es circular en él.
1. Demostremos que no toda relación circular en un conjunto es de equivalencia en él.
2. Averigüemos qué necesita satisfacer una relación circular en un conjunto para ser de equivalencia en él. Demostrémoslo.

[EFO 24.5.2018:2].

Actividad 11.20

Sean R una relación diádica definida en un conjunto X y los predicados

$P \quad :\Leftrightarrow R$ es de equivalencia en X,

$Q_0 \quad :\Leftrightarrow (\forall x \in X)(\exists y \in X)(yRx)$, y

$Q_1 \quad :\Leftrightarrow (\forall x, y, z \in X)(xRy \wedge xRz \rightarrow yRz)$.

Demostremos que $\{P\} \vdash Q_0 \wedge Q_1$.

Actividad 11.21

Sea $X = \{0, 1, 2\}$ y la relación diádica R en 2^X definida por $(\forall U, V \in 2^X)(URV \leftrightarrow U \setminus V = V \setminus U)$. ¿Es R una relación de equivalencia en 2^X?

Actividad 11.22

Sea D_{30} el conjunto de los divisores positivos de 30.

0. Demostremos que la relación de divisibilidad $|$ ordena parcialmente D_{30} y representémosla gráficamente mediante un diagrama de Hasse el conjunto ordenado $(D_{30}; |)$.
1. Hallemos los elementos destacados (cotas, minimales, maximales, ínfimo, supremo, mínimo, máximo) de $\{3, 5, 15\}$ en $(D_{30}; |)$.
2. Hallemos los elementos destacados de D_{30} en $(\mathbb{Z}^+; |)$.

Actividad 11.23

Sean $n \in \mathbb{Z}^+$ y la relación diádica R en $\mathbb{Z}$ definida por $(\forall x, y \in \mathbb{Z})(xRy \leftrightarrow x - y$ es múltiplo de $n)$. Estudiemos si es una relación de equivalencia en $\mathbb{Z}$ y en su caso hallemos el conjunto cociente.

Actividad 11.24

Sean $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ y la relación diádica R en $\mathbb{R}^* \times \mathbb{R}^*$ definida por $(\forall \langle x, y\rangle, \langle z, w\rangle \in \mathbb{R}^* \times \mathbb{R}^*)(\langle x, y\rangle R\langle z, w\rangle \leftrightarrow x \cdot w^2 = z \cdot y^2)$.

0. Demostremos que R es de equivalencia en $\mathbb{R}^* \times \mathbb{R}^*$.
1. Calculemos $[\langle 1, 5\rangle]$ en $(\mathbb{R}^* \times \mathbb{R}^*; R)$.
2. Demostremos que $\langle x, y\rangle R\langle z, w\rangle \leftrightarrow \exists! k \in \mathbb{R}^*, x = kz \wedge y = \pm\sqrt{k}w$.

Actividad 11.25

Sean $X = \{0, 1, 2\}$ y la relación R en 2^X, definida por $(\forall U, V \in 2^X)(URV \leftrightarrow \exists f : U \longrightarrow V$, biyectiva$)$.

0. ¿Es R de equivalencia en 2^X?
1. En caso afirmativo, hallemos la clase de equivalencia de $U \in 2^X$ y el conjunto cociente.

Actividad 11.26

¿Es posible que exista un conjunto X donde la relación diádica R, definida por $(\forall x, y \in X)(xRy$ si, y sólo si, $x^y = y^x)$, sea relación de equivalencia y de orden?

Actividad 11.27

¿Existe algún subconjunto X de $\mathbb{R}$ donde la relación diádica definida por $(\forall x, y \in X)(xRy \leftrightarrow 7 + x = 7y)$ sea relación de equivalencia?

Actividad 11.28

Dado un conjunto parcialmente preordenado $(A; \succsim)$ y una función $f : A \longrightarrow \mathbb{R}$, decimos que f es *isótona* (o, sinónimamente, que *conserva el preorden parcial*) si, y sólo si,

I. $(\forall x, y \in A)(x \succ y \rightarrow f(x) > f(y))$, y
II. $(\forall x, y \in A)(x \sim y \rightarrow f(x) = f(y))$.

Decimos que f es una *representación fiel* del preorden $\succsim$ cuando se satisface que $(\forall x, y \in A)(x \succsim y \leftrightarrow f(x) \geq f(y))$. Demostremos que:

0. si existe una representación fiel de un preorden, entonces éste es fuertemente completo;
1. cualquier función isótona de un preorden fuertemente completo es una representación fiel suya.

Actividad 11.29

Sea la relación diádica $(\forall \langle a, b\rangle, \langle c, d\rangle \in \mathbb{N}^2)(\langle a, b\rangle R \langle c, d\rangle \leftrightarrow (2a+1)2^d \leq (2c+1)2^b)$. Demostremos que es una relación de orden en $\mathbb{N}^2$.

Actividad 11.30

Definimos en $\mathbb{R}^2$: $(\forall \langle a, b\rangle, \langle c, d\rangle \in \mathbb{R}^2)(\langle a, b\rangle * \langle c, d\rangle \leftrightarrow (a \neq c \rightarrow a < c) \wedge (a = c \rightarrow b \leq d))$. Sabemos que $*$ es una relación de orden en $\mathbb{R}^2$, ¿verdad? ¿Es de orden total?

Actividad 11.31

Sea P una relación diádica de preorden, definida en un conjunto A. Definimos en A la relación R por $(\forall x, y \in A)(xRy \leftrightarrow (xPy) \wedge (yPx))$.

0. Demostremos que R es de equivalencia en ${}^{A}/_{R}$.
1. En ${}^{A}/_{R}$ definimos la relación S: $(\forall [x], [y] \in {}^{A}/_{R})([x]S[y] \leftrightarrow xPy)$ (siendo $x \in [x]$, $y \in [y]$). Demostremos que S es una relación de orden en ${}^{A}/_{R}$.
2. ¿Es posible asegurar que S es de orden parcial en A? ¿Y de orden total?

Actividad 11.32

Sea R una relación diádica de preorden parcial definida en un conjunto X. Sea la relación

diádica S definida en X por $(\forall x, y \in S)(xSy \leftrightarrow xRy \wedge yRx)$. Sea la relación diádica $\preccurlyeq$ definida en el conjunto cociente ${}^{X}\!/_{S}$ por $(\forall [x], [y] \in {}^{X}\!/_{S})([x] \preccurlyeq [y] \leftrightarrow xRy)$.

0. Demostremos que S es una relación de equivalencia en X.
1. Demostremos que $\preccurlyeq$ es una relación de orden parcial en ${}^{X}\!/_{S}$.
2. Hallemos las clases de equivalencia en el caso de tratarse del conjunto $\mathbb{Z}$ y la relación de divisibilidad $|$.

[SEP 12.5.2022:3].

Actividad 11.33

¿Es posible asegurar que la relación unión de dos relaciones de equivalencia es una relación de equivalencia? ¿Y la relación unión de dos preórdenes, es necesariamente un preorden?

Actividad 11.34

Sea $X \neq \emptyset$. Sea R una relación diádica de orden en X. Demostremos que, caso de que exista un máximo en X para R, tal máximo es único.

Actividad 11.35

Sea $n \in \mathbb{N} \setminus \{0\}$. En $\mathbb{R}$ definimos la siguiente relación diádica: $(\forall x, y \in \mathbb{R})(xR_n y \leftrightarrow 7^{x-y}$ es múltiplo de $n)$.

0. Si $n = 1$, ¿es R_n de equivalencia o de orden?
1. ¿Puede ser R_n de equivalencia o de orden para algún $n \neq 1$? En caso afirmativo, hallemos todos los n posibles.

Actividad 11.36

Dado un conjunto de algoritmos, establecemos en él la relación diádica «halla la misma solución que». Estudiemos qué propiedades satisface dicha relación diádica de entre las propiedades reflexiva, irreflexiva, simétrica, antisimétrica, asimétrica, transitiva y conexa (esto es, estudiemos cómo estructura dicha relación al conjunto considerado de algoritmos). Si es una equivalencia, ¿cuáles son las clases de equivalencia?; si es una ordenación, ¿de qué tipo?

[AIC 10.4.2018:2Aa], [AIC 10.4.2018:2Ba], [SEL 4:7]. *Cfr.* CÓRDOBA BUENO [176]: ejercicio 1.1 (págs. 6–7).

Actividad 11.37

Sea C un conjunto de programas. Sea $\sim$ la relación diádica definida en C por $(\forall P, Q \in C)(P \sim Q \leftrightarrow t_P + c_Q = c_P + t_Q)$, donde $+$ es la suma habitual entre números reales, t_X es el número de variables temporales del programa $X \in C$ y c_X es el número de estructuras condicionales del programa $X \in C$.

0. Demostremos si $\sim$ satisface o no las propiedades: I, reflexiva; II, simétrica; III, antisimétrica; IV, transitiva, y V, conexa, y digamos: VI, qué tipo de relación es, y por qué.
1. Proporcionemos un ejemplo de conjunto C y considerando $\sim$ actuando en él, mostremos cuáles son las clases de tolerancia, las clases de equivalencia o dibujemos un diagrama de Hasse, dependiendo de que $\sim$ sea una relación de tolerancia, una relación de equivalencia o una ordenación en C.

[EFEC 25.6.2019:2a].

Actividad 11.38

Sea C un conjunto de programas. En dicho conjunto, consideramos que un programa P es de mayor calidad que otro Q, cuestión que designamos por $P \succ Q$, precisamente si es más corto tanto en líneas de código como en número de instrucciones (según $S : P \longrightarrow \mathbb{R}$, una métrica inversa de longitud —$(\forall P, Q \in C)(P \succ Q \leftrightarrow S(P) > S(Q))$—) y menos compleja su estructura (según $\gamma : P \longrightarrow \mathbb{R}$, una métrica de complejidad —$(\forall P, Q \in C)(P \succ Q \leftrightarrow \gamma(P) < \gamma(Q)$—). Estudiemos qué propiedades satisface la relación diádica «ser de mayor calidad que» ($\succ$) de entre las propiedades reflexiva, irreflexiva, simétrica, antisimétrica, asimétrica, transitiva y conexa (esto es, estudiemos cómo estructura dicha relación al conjunto de todos los programas). Si es una equivalencia, ¿cuáles son las clases de equivalencia?; si es una ordenación, ¿de qué tipo?

[SEL 4:8]. *Cfr.* Córdoba Bueno [176]: ejercicio 1.6 (págs. 11–12).

Actividad 11.39

Sea C un conjunto de programas. Sea $\succcurlyeq$ la relación diádica definida en C a partir de las métricas t (n.º variables temporales) y c (n.º de estructuras condicionales), por $(\forall P, Q \in C)(P \succcurlyeq Q \leftrightarrow (t_P < t_Q) \vee ((t_P = t_Q) \wedge (c_P \leq c_Q)))$, esto es, el programa P está relacionado con Q si, y sólo si, el número de variables temporales t_P que usa P es menor que el correspondiente a Q y a igual número de variables temporales si el número de estructuras condicionales c_P presentes en P es menor o igual que el correspondiente a Q.

0. Demostremos si $\succcurlyeq$ satisface o no las propiedades: I, reflexiva; II, simétrica; III, antisimétrica; IV, transitiva, y V, conexa, y digamos: VI, qué tipo de relación es, y por qué.
1. Proporcionemos un ejemplo de conjunto C y considerando $\succcurlyeq$ actuando en él, mostremos cuáles son las clases de tolerancia, las clases de equivalencia o dibujemos un diagrama de Hasse, dependiendo de que $\succcurlyeq$ sea una relación de tolerancia, una relación de equivalencia o una ordenación en C.

Actividad 11.40

Deseamos elegir entre un número finito de programas provenientes de desarrollo basa-

do en componentes. Utilizaremos el índice de reusabilidad por componente de software (RCS), definida por el cociente de numerador el número de componentes reutilizadas y de denominador el número de componentes. Estudiemos qué propiedades satisfacen las relaciones diádicas «tener un mayor RCS que» y «tener el mismo RCS que» de entre las propiedades reflexiva, irreflexiva, simétrica, antisimétrica, asimétrica, transitiva y conexa (esto es, estudiemos cómo estructuran dichas relaciones al conjunto considerado de programas). Si son equivalencias, ¿cuáles son las clases de equivalencia?; si son ordenaciones, ¿de qué tipo?

[SEL 4:9]. *Cfr.* Córdoba Bueno [176]: ejercicio 1.4 (pág. 10).

Actividad 11.41

Consideremos las asignaturas $A_1, A_2, \ldots, A_n$ que estamos preparando para la siguiente convocatoria de exámenes. Para cada una de ellas, consideremos el tiempo medio semanal que dedicamos a su estudio y la calificación final que esperamos obtener en ella. Supongamos que decidimos adoptar la siguiente relación de preferencia: «Preferimos la asignatura A_i a la asignatura A_j si el tiempo medio semanal dedicado al estudio de A_i es menor o igual que el dedicado a A_j y la calificación final que esperamos obtener en A_i es mayor o igual que la que esperamos para A_j».

0. ¿Qué prioridad estableceríamos a la hora de estudiar nuestras asignaturas?
1. Si por cualquier motivo no tuviésemos tiempo para prepararlas todas, ¿cuál o cuáles dejaríamos de estudiar?
2. Estudiemos qué propiedades satisface dicha relación diádica de entre las propiedades reflexiva, irreflexiva, simétrica, antisimétrica, asimétrica, transitiva y conexa (esto es, estudiemos cómo estructura dicha relación al conjunto considerado de asignaturas). Si es una equivalencia, ¿cuáles son las clases de equivalencia?; si es una ordenación, ¿de qué tipo?

[SEL 4:10]. *Cfr.* Córdoba Bueno [176]: ejercicio 1.9 (págs. 17–18).

Con miras a su resolución.— Siendo, por ejemplo, seis las asignaturas, A, I, M, F, R y T, y siendo los criterios de decisión, calificación esperada (ce) y tiempo de preparación esperado (tpe), imaginemos que las puntuaciones que hemos estimado son:

	A	I	M	F	R	T
ce	4	4	2	7	3	9
tpe	3	2	2	1	4	4

Pudiésemos utilizar el artefacto en línea SageMath[46] y el siguiente programita en lenguaje Sage para dibujar el diagrama de Hasse con dos abordajes, manual y «automático».

[46] *Cfr. supra* § 11 (pág. cii de esta edición).

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
# (doc: https://doc.sagemath.org/html/en/reference/combinat/sage/combinat/posets/posets.html)

## # Versión manual
# introduciendo el preorden (copp abrevia conjunto parcialmente preordenado)
copp = Poset({”M”:[”I”,”F”], ”A”:[”I”,”F”], ”I”:[”F”], ”R”:[”A”,”I”,”F”,”T”]})

# dibujando el diagrama de Hasse
copp.plot()

## # Versión «automática» (SageMath genera el preorden).
# asignando las puntuaciones estimadas de los dos criterios (calificación esperada [ce],
# tiempo de preparación estimado [tpe]) para cada asignaturas A, I, M, F, R y T
puntuaciones = {
        ’A’: (4, 3),
        ’I’: (4, 2),
        ’M’: (2, 2),
        ’F’: (7, 1),
        ’R’: (3, 4),
        ’T’: (9, 4)
}
```

```
# definiendo la relación de preferencia bicriterio (ai, aj, asignaturas)
preferencia = [(i, j) for i, ai in puntuaciones.items() for j, aj in puntuaciones.items()
if ai[0] <= aj[0] and ai[1] >= aj[1]]

# generando el preorden parcial
copp = Poset((list(puntuaciones.keys()), preferencia))

# dibujando el diagrama de Hasse
copp.plot()
```

Observemos que en la versión automática hemos definido la preferencia así:

```
# definiendo la relación de preferencia bicriterio (ai, aj, asignaturas)
preferencia = [(i, j) for i, ai in puntuaciones.items() for j, aj in puntuaciones.items()
if ai[0] <= aj[0] and ai[1] >= aj[1]]
```

para que la más preferida, F, quede arriba (de arriba-abajo leeríamos $F \succcurlyeq I \succcurlyeq \ldots$).

Claro que si queremos el diagrama de Hasse, digamos estándar, con el sentido de la relación hacia arriba (que $A\,R\,B$, en este caso, $A \succcurlyeq B$, corresponda a abAjo-arriBa), sería:

```
# definiendo la relación de preferencia bicriterio (ai, aj, asignaturas)
preferencia = [(i, j) for i, ai in puntuaciones.items() for j, aj in puntuaciones.items()
if ai[0] >= aj[0] and ai[1] <= aj[1]]
```

que refleja pura y llanamente nuestra preferencia, a saber, hemos decidido preferir la asignatura con mayor calificación esperada y menor tiempo de preparación estimado (la más preferida, F,

ahora quedaría abajo, de abajo-arriba leeríamos $F \succcurlyeq I \succcurlyeq \ldots$). (Algo similar hubiésemos de hacer con la versión manual).

Actividad 11.42

Sean un conjunto no vacío A y una relación de tolerancia R en A. ¿Es cierto que un subconjunto S de A es una clase de tolerancia precisamente si $\text{im}_R S = S$?

Actividad 11.43

Sea $\mathcal{E} = \{A, B, C, D, G, J, L, M, N, P\}$ un conjunto de nueve entidades determinadas a partir de presentar cuatro cualidades en diferentes grados ($a - e$): $A(b, a, a, b)$, $B(c, e, a, b)$, $C(c, d, b, a)$, $D(a, d, a, b)$, $G(a, d, a, b)$, $J(a, b, c, a)$, $L(b, c, c, a)$, $M(c, a, a, b)$, $N(b, a, a, b)$ y $P(b, b, c, a)$. Se considera la siguiente relación diádica en $\mathcal{E}$: «dos entidades son compatibles si no difieren en más de una de las cuatro cualidades». Esta relación clasifica las entidades en subconjuntos de entidades «compatibles» según dicha relación. Estos subconjuntos se denominan *clases de compatibilidad* o simplemente *vecindades* —por ejemplo, $\{A, M, N\}$ y $\{B, M\}$ son vecindades, ya que A, M y N difieren sólo en la primera cualidad y B y M sólo en la segunda— y al diagrama que representa todas las vecindades, *diagrama de compatibilidades* o *diagrama de vecindades*. Se pide que:

0. estudiemos dicha relación definida en $\mathcal{E}$ (hallemos las diferentes propiedades que satisface [simetría, transitividad, etc.] y todas las vecindades y dibujemos el diagrama de vecindades);
1. hagamos lo mismo para estas otras dos relaciones definidas en $\mathcal{E}$:
    0. «dos entidades son compatibles si no difieren en más de dos de las cuatro cualidades»;
    1. «dos entidades son compatibles si no difieren en más de tres de las cuatro cualidades».

[SEL 4:11]. *Cfr.* Klir, St. Clair y Yuan [177]: § 5.2 *Equivalence and compatibility relations* (págs. 128–132) y ejercicio 6.5 (pág. 141). *Cfr. infra* ejemplo 361 (pág. 682).

Actividad 11.44

Reescribamos las definiciones de las propiedades estudiadas en este capítulo con funciones características. Por ejemplo:

0. Reflexiva: $(\forall x \in C)(\mu_R(x, x) = 1)$
1. Irreflexiva: $(\forall x \in C)(\mu_R(x, x) = 0)$
2. Simétrica: $(\forall x, y \in C)(\mu_R(x, y) \to \mu_R(y, x))$

Actividad 11.45

Sea R una relación diádica y E el conjunto de referencia. Consideremos las siguientes propiedades:

0. $(\forall x, y \in C)(x \neq y \to \mu_R(x, y) \neq \mu_R(y, x) \vee \mu_R(x, y) = \mu_R(y, x) = 0)$
1. $(\exists (x, y) \in C \times C)(x \neq y \to \mu_R(x, y) \neq \mu_R(y, x))$
2. $(\forall (x, y) \in C \times C, \text{con } x \neq y)(\mu_R(x, y) > 0 \to \mu_R(y, x) = 0)$

Para cada una de ellas, discutamos si equivale a alguna de las estudiadas en este capítulo.

Actividad 11.46

En la teoría de los conjuntos borrosos definimos la *transitividad* máx — mín para las relaciones diádicas borrosas como $\mu_R(x, z) \geq \text{máx}_y \text{mín}\{\mu_R(x, y), \mu_R(y, z)\}$. ¿Incluye esta definición como caso particular la transitividad entre conjuntos ordinarios? (Observemos que la operación mín corresponde a $\wedge$ y la operación máx a $\vee$).

Actividad 11.47

En la teoría de los conjuntos borrosos definimos la *transitividad* mín — máx para las relaciones diádicas borrosas como $\mu_R(x, z) \leq \text{mín}_y \text{máx}\{\mu_R(x, y), \mu_R(y, z)\}$. Discutamos si esta propiedad equivale a alguna de las ya estudiadas.

Actividad 11.48

[(Pequeña indagación vía web [*webquest*])] Definimos la *composición* máx — mín de dos relaciones $R_1 \subset X \times Y$ y $R_2 \subset Y \times Z$ por: $\mu_{R_2 \circ R_1} = \sum_y^{\bullet} \mu_{R_1}(x, y) \cdot \mu_{R_2}(y, z)$, donde $\cdot$ es el *producto de* BOOLE y $\sum^{\bullet}$ la *suma de* BOOLE. Interpretemos esta fórmula en el lenguaje habitual de las relaciones ordinarias (sin funciones características).

§ 11.32 Muestra de ejemplos finales

Ejemplo 361

Sea $\mathcal{E} = \{A, B, C, D, G, J, L, M, N, P\}$ un conjunto de diez entes determinados a partir de presentar cuatro cualidades en diferentes grados, del a al e, con $a \prec b \prec c \prec e$: $A(b, a, a, b)$, $B(c, e, a, b)$, $C(c, d, b, a)$, $D(a, d, a, b)$, $G(a, d, a, b)$, $J(a, b, c, a)$, $L(b, c, c, a)$, $M(c, a, a, b)$, $N(b, a, a, b)$ y $P(b, b, c, a)$. Consideremos los siguientes tres casos de relación diádica R definida en $\mathcal{E}$:

0. $(\forall X, Y \in \mathcal{E})\,(X\ R\ Y \leftrightarrow X$ e Y presentan la primera cualidad en el mismo grado);
1. $(\forall X, Y \in \mathcal{E})\,(X(x_1, x_2, x_3, x_4)\ R\ Y(y_1, y_2, y_3, y_4) \leftrightarrow \text{máx}(x_1, x_2) \prec \text{máx}(y_1, y_2) \vee \text{máx}(x_1, x_2) = \text{máx}(y_1, y_2))$;
2. $(\forall X, Y \in \mathcal{E})\,(X\ R\ Y \leftrightarrow X$ e Y no difieren en más de una de las cuatro cualidades).

En cada uno de estos tres casos:

a. averigüemos qué tipo de relación es R y demostremos por qué lo es, estudiando si R satisface o no las siguientes propiedades: I, reflexiva; II, simétrica; III, antisimétrica; IV, transitiva, y V, conexa (fuertemente completa);
b. hallemos las clases de equivalencia, las clases de tolerancia o dibujemos un diagrama de Hasse, dependiendo de que R sea una relación de equivalencia, una relación de tolerancia o una relación de orden en $\mathcal{E}$.

[EFO 12.6.2020:1b (p.h.e.c.)]. *Cfr. supra* actividad 11.43 (pág. 680).

Resolución.— Cada ente X tiene cuatro cualidades, $X(cual_1, cual_2, cual_3, cual_4)$, y cada cualidad la posee en diferentes grados, esto es, por ejemplo, como $b \prec c$, el ente $A(b, a, a, b)$ posee la primera cualidad en grado menor que la posee el ente $B(c, e, a, b)$.

Caso 0.

Sea R la relación diádica definida en $\mathcal{E}$ por:
$(\forall X, Y \in \mathcal{E})\,(X\ R\ Y \leftrightarrow X$ e Y presentan la primera cualidad en el mismo grado).

a. Dados cualesquiera entes $X(x_1, x_2, x_3, x_4)$ e $Y(y_1, y_2, y_3, y_4)$ de $\mathcal{E}$:

   I. si desconocemos cómo se relaciona d con el resto de grados mediante $\prec$, no pudiésemos calcular el máximo si uno de los argumentos es d y no habría resultado, en otras palabras, no pudiésemos aceptar un argumento del estilo de «sea el que sea el resultado, siempre se tendrá $x = x$ o $d = d$» ya que no habría forma de llegar a esas igualdades a través del cálculo del máximo con su definición clásica. Suponiendo, pues, que se satisface que $a \prec b \prec c \prec d \prec e$, y siendo $=$ una relación de equivalencia en $\{a, b, c, d, e\}$ y, por tanto,

reflexiva, entonces, sí es R reflexiva en $\mathcal{E}$, pues cualquier ente posee las cuatro cualidades en el mismo grado que él mismo y en particular la primera;

II. es simétrica en $\mathcal{E}$, pues afirmar que el ente X posee la primera cualidad en el mismo grado que la posee el ente Y (esto es, $x_1 = y_1$) es equivalente a afirmar que el ente Y posee la primera cualidad en el mismo grado que la posee el ente X (esto es, $y_1 = x_1$);

III. no es antisimétrica, pues, por ejemplo, $A(b, a, a, b)$ y $L(b, c, c, a)$ están mutuamente relacionados por R pero $A(b, a, a, b)$ no es $L(b, c, c, a)$;

IV. suponiendo que $=$ una relación de equivalencia en $\{a, b, c, d, e\}$ y, por tanto, transitiva, entonces sí es R transitiva en $\mathcal{E}$, pues si los entes X e Y presentan la primera cualidad en el mismo grado (esto es, $x_1 = y_1$) y los entes Y y Z presentan la primera cualidad en el mismo grado (esto es, $y_1 = z_1$), entonces, los entes X y Z presentan la primera cualidad en el mismo grado (esto es, $x_1 = z_1$), en otras palabras, de la transitiva de $=$ en $\{a, b, c, d, e\}$ se deduce la transitiva de R en $\mathcal{E}$;

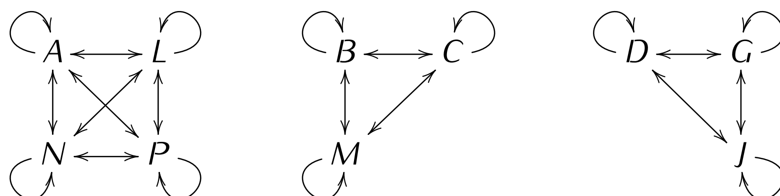
V. no es conexa en $\mathcal{E}$, ya que, por ejemplo, $A(b, a, a, b) \not R B(c, e, a, b)$ y $B(c, e, a, b) \not R A(b, a, a, b)$.

Caso de satisfacer R las propiedades reflexiva, simétrica y transitiva en $\mathcal{E}$, se diría que R es una relación de equivalencia en $\mathcal{E}$.

b. La definición de los entes en función del grado de posesión de la primera cualidad es

	$cual_1$
A	b
B	c
C	c
D	a
G	a
J	a
L	b
M	c
N	b
P	b

Identificamos tres clases de equivalencia,
$[A] = \{x \in \mathcal{E}, x\ R\ A\} = \{A, L, N, P\}$ (entes que poseen la 1.ª cualidad en grado b),
$[B] = \{x \in \mathcal{E}, x\ R\ B\} = \{B, C, M\}$ (entes que poseen la 1.ª cualidad en grado c), y
$[D] = \{x \in \mathcal{E}, x\ R\ D\} = \{D, G, J\}$ (entes que poseen la 1.ª cualidad en grado a).
Como es sabido y seríamos capaces de demostrar, el conjunto cociente $\mathcal{E}/R = \{[A], [B], [D]\}$ es una partición de $\mathcal{E}$. Representamos gráficamente la relación R en $\mathcal{E}$ y esta partición:



Caso 1.

Sea R la relación diádica definida en $\mathcal{E}$ por:
$(\forall X, Y \in \mathcal{E})\ (X(x_1, x_2, x_3, x_4)\ R\ Y(y_1, y_2, y_3, y_4) \leftrightarrow \text{máx}(x_1, x_2) \prec \text{máx}(y_1, y_2) \lor \text{máx}(x_1, x_2) = \text{máx}(y_1, y_2))$.

a. Dados cualesquiera entes $X(x_1, x_2, x_3, x_4)$ e $Y(y_1, y_2, y_3, y_4)$ de $\mathcal{E}$:

I. Si desconocemos cómo se relaciona d con el resto de grados mediante $\prec$, no pudiésemos calcular el máximo si uno de los argumentos es d y no habría resultado, en otras palabras, no pudiésemos aceptar un argumento del estilo de «sea el que sea el resultado, siempre se tendrá $x = x$ o $d = d$» ya que no habría forma de llegar a esas igualdades a través del cálculo del máximo con su definición clásica. Suponiendo, pues, que se satisface que $a \prec b \prec c \prec d \prec e$, y siendo $=$ una relación de equivalencia en $\{a, b, c, d, e\}$ y, por tanto, reflexiva, entonces, sí es R reflexiva en $\mathcal{E}$, pues para cualquier $X(x_1, x_2, x_3, x_4) \in \mathcal{E}$,

$$\begin{aligned}\text{máx}(x_1, x_2) = \text{máx}(x_1, x_2) &\rightarrow (\text{máx}(x_1, x_2) \prec \text{máx}(x_1, x_2) \lor \text{máx}(x_1, x_2) = \text{máx}(x_1, x_2)) \\ &\rightarrow X(x_1, x_2, x_3, x_4)\ R\ Y(y_1, y_2, y_3, y_4);\end{aligned}$$

II. no es simétrica en $\mathcal{E}$, pues, por ejemplo,

$$\begin{gathered}\text{máx}(b, a) = b \prec e = \text{máx}(c, e) \rightarrow A(b, a, a, b)\ R\ B(c, e, a, b) \\ \land \\ \begin{pmatrix}\text{máx}(c, e) = e \not\prec b = \text{máx}(b, a) \\ \land \\ \text{máx}(c, e) = e \neq b = \text{máx}(b, a)\end{pmatrix} \rightarrow B(c, e, a, b) \not{R}\, A(b, a, a, b);\end{gathered}$$

III. no es antisimétrica en $\mathcal{E}$, pues, por ejemplo, $A(b, a, a, b) \neq J(a, b, c, a)$ a pesar de que

$$\begin{gathered}\text{máx}(b, a) = b = \text{máx}(a, b) \rightarrow A(b, a, a, b)\ R\ J(a, b, c, a) \\ \land \\ \text{máx}(a, b) = b = \text{máx}(b, a) \rightarrow J(a, b, c, a)\ R\ A(b, a, a, b);\end{gathered}$$

IV. $=$ es una relación de equivalencia en $\{a, b, c, d, e\}$ y, por tanto, transitiva; si $\prec$ es transitiva en $\{a, b, c, d, e\}$ y $a \prec b \prec c \prec d \prec e$, entonces, R es transitiva en $\mathcal{E}$, ya que notando por $X \prec Y \leftrightarrow \text{máx}(x_1, x_2) \prec \text{máx}(y_1, y_2)$ y $X \approx Y \leftrightarrow \text{máx}(x_1, x_2) = \text{máx}(y_1, y_2)$, se tiene

que $X\,R\,Y \leftrightarrow X \prec Y \wedge X \approx Y$, y

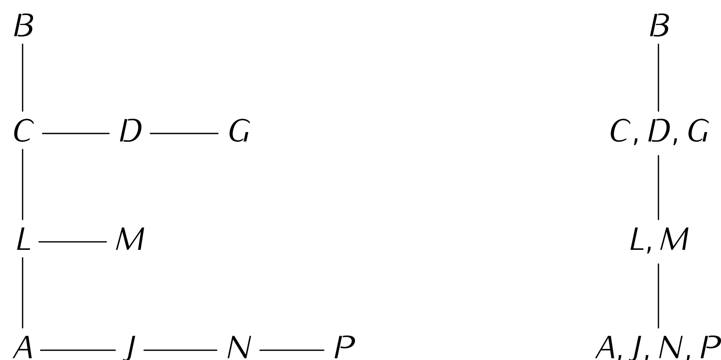
$$X\,R\,Y \;\wedge\; Y\,R\,Z \rightarrow \begin{pmatrix} X \prec Y \wedge Y \prec Z \rightarrow X \prec Z \\ \vee \\ X \prec Y \wedge Y = Z \rightarrow X \prec Z \\ \vee \\ X \approx Y \wedge Y \prec Z \rightarrow X \prec Z \\ \vee \\ X \approx Y \wedge Y \approx Z \rightarrow X \approx Z \end{pmatrix} \rightarrow X\,R\,Z;$$

es cierto por la transitividad de $\prec$ y $=$ en $\{a, b, c, d, e\}$; sin embargo, si $\prec$ no satisface la transitiva en $\{a, b, c, d, e\}$ o desconocemos cómo se relaciona d con el resto de grados mediante $\prec$, R no es posible asegurar que R sea transitiva en $\mathcal{E}$;

v. la relación de igualdad $=$ es conexa (fuertemente completa) en $\{a, b, c, d, e\}$; si $\prec$ es conexa en $\{a, b, c, d, e\}$ y $a \prec b \prec c \prec d \prec e$, entonces, R es conexa en $\mathcal{E}$; sin embargo, si $\prec$ no es conexa en $\{a, b, c, d, e\}$ o desconocemos cómo se relaciona d con el resto de grados mediante $\prec$, no es posible asegurar que R sea conexa en $\mathcal{E}$.

Caso de satisfacer R las propiedades reflexiva, transitiva y conexa en $\mathcal{E}$, se diría que R es una relación de preorden en $\mathcal{E}$.

b. En tal caso, dos formas habituales de representar como diagrama de Hasse el preorden R en $\mathcal{E}$ son



representando las aristas horizontales en el primero la simetría (L—M significa $L\,R\,M \wedge M\,R\,L$) y siendo los nodos en el segundo las clases de equivalencia de la subrelación de equivalencia de R (las 4 clases de equivalencia generadas entre los elementos que satisfacen la simétrica). Observemos que como tales diagramas de Hasse, en estas rerpresentaciones se asume que R satisface las propiedades reflexiva y transitiva, por lo que, por ejemplo, en el primero, $J\,R\,L$ ya que $J\,R\,A$ y $A\,R\,L$ y ser R transitiva.

Caso 2.

Sea R la relación diádica definida en $\mathcal{E}$ por:
$(\forall X, Y \in \mathcal{E})\,(X\ R\ Y \leftrightarrow X$ e Y no difieren en más de una de las cuatro cualidades).

a. La definición de los entes en función del grado de posesión de las cualidades es

	$cual_1$	$cual_2$	$cual_3$	$cual_4$
A	b	a	a	b
B	c	e	a	b
C	c	d	b	a
D	a	d	a	b
G	a	d	a	b
J	a	b	c	a
L	b	c	c	a
M	c	a	a	b
N	b	a	a	b
P	b	b	c	a

La relación R actuando en $\mathcal{E}$, expresada en forma de matriz binaria (1 significa que los entes del par asociado son compatibles y 0 que no lo son), es

	A	B	C	D	G	J	L	M	N	P
A	1	0	0	0	0	0	0	1	1	0
B	0	1	0	0	0	0	0	1	0	0
C	0	0	1	0	0	0	0	0	0	0
D	0	0	0	1	1	0	0	0	0	0
G	0	0	0	1	1	0	0	0	0	0
J	0	0	0	0	0	1	0	0	0	1
L	0	0	0	0	0	0	1	0	0	1
M	1	1	0	0	0	0	0	1	0	0
N	1	0	0	0	0	0	0	0	1	0
P	0	0	0	0	0	1	1	0	0	1

I. es reflexiva en $\mathcal{E}$, pues cualquier ente posee las cuatro cualidades en el mismo grado que él mismo, así que un ente y él mismo no difieren en más de una de las cuatro cualidades (puede observarse que la diagonal de la matriz es 1);

II. sí es simétrica en $\mathcal{E}$, pues decir que el ente X no difiere en más de una de las cuatro cualidades del ente Y es equivalente a decir que el ente Y no difiere en más de una de las cuatro cualidades del ente X (la matriz anterior es simétrica respecto de la diagonal principal);

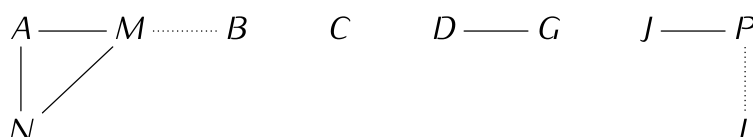
III. no es antisimétrica en $\mathcal{E}$, pues, por ejemplo, $A(b,a,a,b)\ R\ M(c,a,a,b)$ y $M(c,a,a,b)\ R\ A(b,a,a,b)$ pero $A \neq M$;

IV. no es transitiva en $\mathcal{E}$, pues, por ejemplo, $A(b,a,a,b)\ R\ M(c,a,a,b)$ y $M(c,a,a,b)\ R\ B(c,e,a,b)$, pero $A \not R B$;

V. no es conexa en $\mathcal{E}$, pues, por ejemplo, $A(b,a,a,b) \not R B(c,e,a,b)$.

Al satisfacer las propiedades reflexiva y simétrica, R es una relación de tolerancia (compatibilidad) en $\mathcal{E}$.

b. La relación R actuando en $\mathcal{E}$ induce las siguientes clases de tolerancia: $\emptyset$, $\{A\}$, $\{B\}$, $\{C\}$, $\{D\}$, $\{G\}$, $\{J\}$, $\{L\}$, $\{M\}$, $\{N\}$, $\{P\}$, $\{A, M\}$, $\{A, N\}$, $\{B, M\}$, $\{D, G\}$, $\{J, P\}$, $\{L, P\}$, $\{M, N\}$ y $\{A, M, N\}$. Seis de ellas no están contenidas en ninguna otra clase de tolerancia, son las clases maximales de tolerancia,$\{A, M, N\}$, $\{B, M\}$, $\{C\}$, $\{D, G\}$, $\{J, P\}$ y $\{L, P\}$, que forman un recubrimiento de $\mathcal{E}$. Una posible representación gráfica sería la siguiente, donde la línea continua (—) expresa que los extremos que une están en la misma clase de tolerancia (esto es, que dichos entes son compatibles según el concepto de compatibilidad definido por R) y una discontinua $(\cdots)$ que no lo son. Así, hablando de compatibilidad, en vez de tolerancia, así, en ella vemos que A, M y N son compatibles de acuerdo con dicho concepto de compatibilidad, y M (pero no así ni A ni N) es también compatible con B, y también J y P son compatibles y P (pero no J) es también compatible con L.



■

§ 11.33 Bibliografía

- Para una primera aproximación:

[145] José García García y Manuel López Pellicer. *Álgebra lineal y geometría: curso teórico-práctico*. Marfil, Alcoy, Hoya de Alcoy, Alicante (ES-A), España, 8.ª ed., 1992.

[146] Armando Óscar Rojo. *Álgebra I*. El Ateneo, Buenos Aires (AR-C), Argentina, 1986. ©TDR.

- Para estudiar, practicar y saber más:

[147] Herbert Bruce Enderton. *Elements of Set Theory*. Academic Press, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1977.

[149] Józef Maria Bocheński. *Compendio de lógica matemática*. Colección Lógica y Teoría de la Ciencia. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1982. Traducido del inglés *A Précis of Mathematical Logic* (1959), traducido a su vez de *Précis de logique mathématique* (1948), Bussum, North Holland: F. G. Kroonder.

[176] Miguel Córdoba Bueno. *La Toma de decisiones en la práctica*. Delta Publicaciones Universitarias, 2005.

[177] George Jiří Klir, Ute H. St. Clair y Bo Yuan. *Fuzzy set theory: foundations and applications*. Prentice Hall, Upper Saddle River, Nueva Jersey (US-NJ), Estados Unidos de América, 1997.

- Y más:

[140] Máximo Anzola González y José Ramón Caruncho Castro. *Problemas de álgebra. Tomo 1: Conjuntos - Grupos*. Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1981. ©TDR.

[144] Agustín de la Villa Cuenca. *Problemas de Álgebra (con esquemas teóricos)*. CLAGSA, Madrid, Comunidad de Madrid (ES-M), España, 4.ª ed., 2010. ©TDR.

- Para profundizar, acullá:

[142] José Antonio Alonso Jiménez, Joaquín Borrego Díaz, Mario de Jesús Pérez Jiménez y José Luis Ruiz Reina. *Curso Práctico de Teoría de Conjuntos*. La Ñ, Sevilla, Andalucía (ES-AN), España, 1998.

- Sin olvidar a los recomendados dedicados a la matemática discreta:

[32] Félix García Merayo. *Matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 2015.

[141] John Kenneth Truss. *Discrete mathematics for computer scientists*. Addison-Wesley, Bungay, Suffolk (GB-SFK), Reino Unido, 1991.

[150] Félix García Merayo, Gregorio Hernández Peñalver y Antonio Nevot Luna. *Problemas resueltos de matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 2018.

[151] Kenneth Howard Rosen. *Matemática discreta y sus aplicaciones*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 5.ª ed., 2004. (La 5.ª edición es la última en español).

[152] Kenneth Howard Rosen. *Discrete Mathematics and its Applications*. McGraw-Hill, Nueva York, Nueva York (US-NY), Estados Unidos de América, 7.ª ed., 2012.

[153] Francisco José González Gutiérrez. *Apuntes de Matemática Discreta*. El autor, Cádiz, Andalucía (ES-AN), España, 2004.

[154] Carlos García Gómez, Josep María López Besora y Dolors Puigjaner Riba. *Matemática discreta*. Pearson Educación, Madrid, Comunidad de Madrid (ES-M), España, 2002.

[155] Ralph Peter Grimaldi. *Matemáticas discreta y combinatoria*. Addison-Wesley Iberoamericana, Wilmington, New Castle, Delaware (US-DE), Estados Unidos de América, 3.ª ed., 1997.

[124] Jiří Matoušek y Jaroslav Nešetřil. *Invitación a la matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2008.

[156] Juan Carlos Ferrando Pérez y Valentín Gregori Gregori. *Matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2.ª ed., 2012.

[157] Kenneth Allen Ross y Charles Richard Bowers Wright. *Matemáticas discretas*. Prentice-Hall Hispanoamericana, Naucalpan de Juárez, Estado Libre y Soberano de México (MX-MEX), Estados Unidos Mexicanos, 2.ª ed., 1990.

[158] Richard Johnsonbaugh. *Discrete Mathematics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 8.ª ed., 2018.

Capítulo 12

Lógica de funciones

Una unidad (entidad, objeto) procede de un acto de distinción. Recíprocamente, siempre que nos referimos a una unidad en nuestras descripciones, implícitamente lo hacemos a la operación de distinción que la define y la hace posible.

(Humberto Maturana y Francisco Varela. *El árbol del conocimiento*).

Como decíamos al presentar la lógica de clases, estudiar qué pueden hacer (cómo se «comportan») las entidades en relación con otras entidades o colecciones, es un objetivo de la lógica de funciones. Éstas son esenciales en la construcción de modelos matemáticos para representar, investigar y resolver numerosas situaciones que acaecen en la ciencia experimental y en la vida en general: en una o más variables —protagonistas éstas, por ejemplo, en la toma de decisión multicriterio—; ecuaciones diferenciales y ecuaciones en diferencias, habilitadoras de modelos continuos y discretos de dinámica de poblaciones, de expansión de una enfermedad; y más, destacando los modelos probabilísticos, y entre éstos los bayesianos[○], a su vez copartícipes en la cimentación de la actual manera de crear la inteligencia artificial y de bregar con ella.

[○] Si nos inquietase el mundo cuántico, pudiésemos ver una extensión de los modelos probabilísticos bayesianos a éste en: Ge Bai, Francesco Buscemi y Valerio Scarani. Quantum Bayes' Rule and Petz Transpose Map from the Minimum Change Principle, *Physical Review Letters, 135,090203*, 28 de agosto de 2025, https://doi.org/10.1103/5n4p-bxhm.

§ 12.0 Correspondencia, función y aplicación

Definición 12.0.— Una *correspondencia* es una relación. Dados dos conjuntos X y Y, una relación $R \subseteq X \times Y$ y un par ordenado $\langle x, y\rangle \in R$, decimos que y es la *imagen* o el valor de x por R (también decimos de x que es la *antiimagen* de y) y este hecho lo representamos por $y = R(x)$. En este ámbito se representa la propia correspondencia por $R : X \longrightarrow Y$; afirmar aquí que $y = R(x)$ equivale a afirmar que $\langle x, y\rangle \in R$, en la vista de R como relación.

Observación 12.0.0.— Debemos a Leibniz (1646–1716) el nombre de función, con un sentido muy parecido al que usamos hoy. Jean Bernoulli (1667–1748) experimentó con varias notaciones, de las que la más parecida a la actual es ϕx. Fue Euler (1707–1783) quien en la revista de la Academia de San Petersburgo, *Commentarii AcademiæScientiarum Imperialis Petropolitanæ*, de 1734–1735, utilizó la notación $f(x)$ para representar una función de x.

Las definiciones establecidas en § 11.0 (pág. 592 de esta edición) para relaciones se reescriben para correspondencias.

Así, dados dos conjuntos X e Y y una correspondencia $f : X \longrightarrow Y$, se denomina:

- *conjunto de partida* (o *conjunto inicial* o *predominio*) de f al conjunto X;
- *conjunto de llegada* (o *conjunto final* o *codominio*) de f al conjunto Y;
- *dominio* (o, sinónimamente, *conjunto original*, *conjunto de orígenes* o *imagen conversa*) de f al conjunto $\operatorname{dom} f = \{x \in X : \exists y \in Y, y = f(x)\}$;
- *rango* (o, sinónimamente, *conjunto imagen*, *imagen*, *conjunto de imágenes*, *contradominio*, *dominio converso* o *recorrido*) de f al conjunto $\operatorname{ran} f = \{y \in Y : \exists x \in X, y = f(x)\}$;
- *campo* de f al conjunto $\operatorname{cam} f = \operatorname{dom} f \cup \operatorname{ran} f$;
- *grafo* de f a la propia función vista como conjunto de pares ordenados, es decir, al conjunto $\{\langle x, y\rangle : y = f(x)\}$ que pudiésemos designar por f o por G_f si quisiésemos destacar que una relación f queda determinada cuando se conoce la terna $\langle X, Y, G_f\rangle$ (en otras palabras, una correspondencia f es una terna $\langle X, Y, G_f\rangle$ donde G_f es un subconjunto de $X \times Y$ —G_f es la relación diádica que se identifica con f—);
- $y \in Y$ es un *elemento imagen* de $x \in X$ precisamente si $\langle x, y\rangle \in G_f$;
- el *conjunto imagen* de $S \subseteq X$ es $\{y \in Y : (\exists x \in S)(\langle x, y\rangle \in G_f)\}$;
- $x \in X$ es un *elemento origen* (o *elemento preimagen*) de $y \in Y$ precisamente si $\langle x, y\rangle \in G_f$;
- el *conjunto origen* (o *conjunto preimagen*) de $T \subseteq Y$ es $\{x \in X : (\exists y \in T)(\langle x, y\rangle \in G_f)\}$.

Definición 12.1.— Decimos que una correspondencia $f : X \longrightarrow Y$ es una *función* precisamente si es una relación funcional, esto es, si asigna como mucho un elemento de ran f a cada elemento de dom f; en otras palabras, la imagen de todo elemento de dom f es un subconjunto unitario de Y.

Imagen monocromática discreta

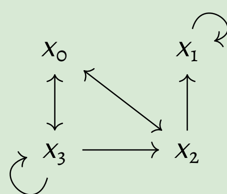
Una *imagen monocromática discreta* es una función $I : \mathbb{Z} \times \mathbb{Z} \longrightarrow [0, n] \cap \mathbb{N}$, siendo $\langle x, y \rangle \in \mathbb{Z} \times \mathbb{Z}$ las *coordenadas* de un punto e $I(x, y)$ su *grado de gris*. Una *operación de procesamiento de imagen* es una función que transforma una imagen I en otra J. Por ejemplo, con las operaciones de *segmentación* se consiguen diferenciar detalles en una imagen. Una de ellas es la operación de *binarización* (o, sinónimamente, *umbralización*), designémosla por B, definida por $B(x, y) = 0$, si $I(x, y) < T$ y $B(x, y) = 1$, si $T \leq I(x, y)$; a T se le conoce como *umbral de binarización*. Pudiese haber dos umbrales, uno inferior T_i y el otro superior T_s: $B(x, y) = 0$, si $I(x, y) \notin [T_i, T_s]$ y $B(x, y) = 1$, si $I(x, y) \in [T_i, T_s]$. El *histograma* de una imagen representa el número de puntos cuyos grados de gris están comprendidos entre T_i y T_s; dicho histograma es la función $H : [T_i, T_s] \longrightarrow \mathbb{N}$, definida por $H(t) \leftrightharpoons$ número de puntos cuyo grado de gris es t.

Si los conjuntos son iguales, decimos que es una *endofunción*.

A la endofunción $id_X : X \longrightarrow X$, definida por $id_X(x) = x$, para todo $x \in X$, la denominamos *función identidad* en X y no es más que la *relación identidad* I_X en X.

Ejemplo 362

Definamos el siguiente grafo dirigido como un par ordenado de un conjunto y una función.



Resolución.— En efecto, definámoslo como el par ordenado $\langle K, \Gamma \rangle$, donde K es el conjunto de orígenes $K = \{x_0, x_1, x_2, x_3\}$ y $\Gamma : K \longrightarrow 2^K$ es la función definida por: $\Gamma(x_0) = \{x_2, x_3\}$, $\Gamma(x_1) = \{x_1\}$, $\Gamma(x_2) = \{x_0, x_1\}$ y $\Gamma(x_3) = \{x_0, x_2, x_3\}$. ■

Definición 12.2.— Decimos que una función $f : X \longrightarrow Y$ es una *aplicación* precisamente si $\mathrm{dom}(f) = X$. En otras palabras, una aplicación $f : X \longrightarrow Y$ es una relación funcional cuyo dominio es X y cuyo rango es un subconjunto de Y. Esto obliga a que para cualquier $x \in X$, existe un

único $y \in Y$ tal que $\langle x, y\rangle \in G_f$, escribiéndose esto último $y = f(x)$, como ya hemos dicho. En resumen, $f : X \longrightarrow Y$ es una aplicación $\leftrightharpoons$ 0.º ∧ 1.º ∧ 2.º, donde:

0.º, $\operatorname{dom} f = X$;

1.º, $\operatorname{ran} f \subseteq Y$, y

2.º, $(\forall x \in X)\,(\forall y, z \in Y)\,(y = f(x) \wedge z = f(x) \rightarrow y = z)$.

Teorema 12.0

$f : X \longrightarrow Y$ es una aplicación si, y sólo si, $(\forall x \in X)(\exists! y \in Y)(f(x) = y)$.

Ejemplo 363 (Inclusión y pertenencia no son relaciones funcionales)

Las siguientes correspondencias f y $f_\subseteq$ intentan recoger la idea de la relación de inclusión, que como sabemos no es funcional. La primera no es función, mientras que la segunda es aplicación.

0. Dado un conjunto C, la correspondencia $f : 2^C \longrightarrow 2^C$, definida $\forall X, Y \in 2^C$ por $f(X) = Y \leftrightarrow X \subseteq Y$, no es una función.

1. Dado un conjunto C, la correspondencia $f_\subseteq : 2^C \times 2^C \longrightarrow \{0, 1\}$, definida $\forall\langle X, Y\rangle \in 2^C \times 2^C$ por $f_\subseteq(X, Y) = 0$ si $X \nsubseteq Y$ y $f_\subseteq(X, Y) = 1$ si $X \subseteq Y$, es una aplicación.

Algo similar ocurre con la pertenencia.

2. Dado un conjunto C, la correspondencia $g : C \longrightarrow 2^C$, definida $\forall x \in C, \forall Y \in 2^C$, por $m(x) = Y \leftrightarrow x \in Y$, no es una función.

3. Dado un conjunto C, la correspondencia $g_\in : C \times 2^C \longrightarrow \{0, 1\}$, definida $\forall\langle x, Y\rangle \in C \times 2^C$ por $g_\in(x, Y) = 0$ si $x \notin Y$ y $g_\in(x, Y) = 1$ si $x \in Y$, es una aplicación.

Observación 12.0.1.— En el ámbito del Análisis Matemático y del Cálculo, a las aplicaciones se les denomina *funciones totales*. A veces, para insistir en el carácter no total de una función decimos que es una *función parcial*. Si sólo decimos que es una función, se trata de una función parcial.

Definición 12.3.— Sean X, Y conjuntos y $f, g : X \longrightarrow Y$ dos funciones tales que $\operatorname{dom} f = \operatorname{dom} g$. Entonces decimos que f y g son *iguales* en $\operatorname{dom} f$ precisamente si $\forall x \in \operatorname{dom} f$, $f(x) = g(x)$.

Observación 12.0.2.— Similarmente a lo visto en el ejemplo 363 (pág. 693 de esta edición), dado un conjunto C, es posible hablar de la aplicación $f_= : 2^C \times 2^C \longrightarrow \{0, 1\}$, definida $\forall\langle X, Y\rangle \in 2^C \times 2^C$ por $f_=(X, Y) = 0$ si $X \neq Y$ y $f_=(X, Y) = 1$ si $X = Y$.

Operaciones de conjuntos en lenguajes de programación

Estas aplicaciones se utilizan en múltiples ámbitos con lenguajes propios, por ejemplo, como operaciones de conjuntos en R. Por ejemplo, $f_{=}(X, Y)$ mediante la instrucción `setequal(X,Y)` y $g_{\in}(x, Y)$ mediante `X %in% Y`.

Para $f_{\subseteq}(X, Y)$ no existe una instrucción específica, pero pudiésemos utilizar `setequal(X,intersect(X,Y))` o bien `all(X %in% Y)`.

R también tiene instrucciones para la unión y la diferencia: `union(X,Y)` y `setdiff(X,Y)`, respectivamente.

§ 12.1 Inyectividad, sobreyectividad y biyectividad

Definición 12.4.— Sean X, Y conjuntos y $f : X \longrightarrow Y$ una función. Entonces decimos que:

0. f es *inyectiva* precisamente si lo es como relación funcional, es decir, si, y sólo si, todo elemento imagen lo es exactamente de un único elemento original, esto es, precisamente si $(\forall x, y \in X)(f(x) = f(y) \to x = y)$.
1. f es *sobreyectiva* (suprayectiva o exhaustiva) precisamente si $\operatorname{ran} f = Y$, es decir, precisamente si todo elemento del conjunto final es imagen de algún elemento del conjunto inicial, esto es, si, y sólo si, $\forall y \in Y, \exists x \in X, f(x) = y$.
2. f es *biyectiva* precisamente si es inyectiva y sobreyectiva.

Teorema 12.1 (Caracterización de la biyectividad)
Sean X, Y conjuntos y $f : X \longrightarrow Y$ una función. Entonces:

$$f \text{ es biyectiva si, y sólo si, } \forall y \in Y, \exists! x \in X, f(x) = y.$$

§ 12.2 Composición de funciones

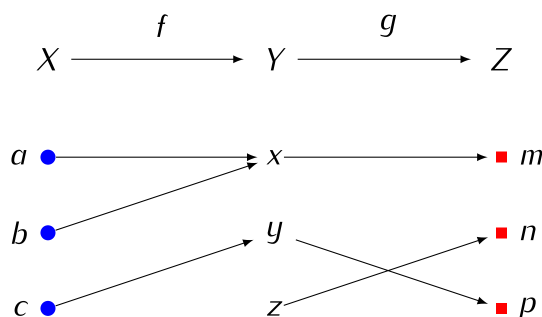
Definición 12.5.— Sean X, Y, Z conjuntos y $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ funciones tales que $\operatorname{im}(f) \subseteq \operatorname{dom}(g)$. Definimos la *composición* de f y g, como $g \circ f : X \longrightarrow Z$, $(g \circ f)(x) = g(f(x))$.

Teorema 12.2
Dados X, Y, Z conjuntos y $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ funciones tales que $\operatorname{im}(f) \subseteq \operatorname{dom}(g)$, la composición $g \circ f$ es una función, la *función compuesta* de f y g.

Ejemplo 364

Sean las funciones $f : \{a, b, c\} \longrightarrow \{x, y\}$ y $g : \{x, y\} \longrightarrow \{m, n, p\}$ definidas respectivamente por $f(a) = f(b) = x$, $f(c) = y$, y por $g(x) = m$, $g(y) = p$, $g(z) = n$. Esfudiemos la función compuesta de f y g.

Resolución.— Gráficamente:



Observamos que $\operatorname{dom} f = \{a, b, c\}$, $\operatorname{im} f = \{x, y\} \subseteq \{x, y, z\} = \operatorname{dom} g$, $\operatorname{im} g = \{m, n, p\}$, que $\operatorname{im} f \subseteq \operatorname{dom} g$ y que $\operatorname{dom}(g \circ f) = \{a, b, c\}$ e $\operatorname{im}(g \circ f) = \{m, p\}$ y que $(g \circ f)(a) = g(f(a)) = g(x) = m$, $(g \circ f)(b) = g(f(b)) = g(x) = m$, $(g \circ f)(c) = g(f(c)) = g(y) = p$. ∎

Observación 12.2.0.— Se dice a veces que X *determina funcionalmente* Z a través de Y (o, sinónimamente, que Z *depende funcionalmente* de X a través de Y).

Fusión de dos conjuntos de datos

Cuando en programación tenemos dos conjuntos de datos correspondientes a las mismas variables, es admisible usar los identificadores de dichas variables como una variable común para fusionar ambos conjuntos. Imaginemos que los conjuntos de datos son $\{\langle 0, f(0)\rangle, \langle 1, f(1)\rangle, \ldots, \langle n, f(n)\rangle\}$ y $\{\langle 0, g(0)\rangle, \langle 1, g(1)\rangle, \ldots, \langle n, g(n)\rangle\}$, entonces la fusión es el conjunto de datos $\{\langle 0, f(0), g(0)\rangle, \langle 1, f(1), g(1)\rangle, \ldots, \langle n, f(n), g(n)\rangle\}$.

Por ejemplo, $n + 1$ personas, $f(i)$ la edad de la persona i y $g(i)$ el peso de la persona i y este identificador i de la persona desde $i = 0$ a n. Un camino matemático utilizando la composición para este último ejemplo pudiese ser el siguiente, tomando $I = \{0, 1, \ldots, n\}$, $X = Y = \mathbb{N}$: $f : I \longrightarrow X, x \longmapsto f(x)$; $g : I \longrightarrow Y, x \longmapsto g(x)$; $g_2 : I \longrightarrow X \times Y, x \longmapsto \langle x, g(x)\rangle$ (esta g_2 exige que $I \subseteq X$); $g_2 \circ f : I \longrightarrow X \times Y$, $(g_2 \circ f)(x) = \langle f(x), g(x)\rangle$.

Teorema 12.3 (Propiedades)
Sean W, X, Y, Z conjuntos y $f : W \longrightarrow X$, $g : X \longrightarrow Y$ y $h : Y \longrightarrow Z$ funciones tales que $\mathrm{im}(f) \subseteq \mathrm{dom}(g)$ y $\mathrm{im}(g) \subseteq \mathrm{dom}(h)$; entonces:

0. $h \circ (g \circ f) = (h \circ g) \circ f$ (asociatividad de $\circ$).
1. si f, g son inyectivas, entonces $g \circ f$ es inyectiva.
2. si f, g son sobreyectivas, entonces $g \circ f$ es sobreyectiva.
3. si f, g son biyectivas, entonces $g \circ f$ es biyectiva.

Observación 12.2.1.— La composición de funciones no es conmutativa.

§ 12.3 Inversa o recíproca

Sean $X = \{0\}$, $Y = \{0, 1\}$ y la relación $R = \{\langle 0, 0\rangle, \langle 0, 1\rangle\}$. Surge un problema al plantear su reescritura como correspondencia; ¿qué escribimos, $R : X \longrightarrow Y$ definida por $R(0) = 0$ y $R(0) = 1$?, ¿o no sería mejor $R : X \longrightarrow 2^Y$ definida por $R(0) = \{0, 1\}$? Pero entonces parece que no estemos hablando de una correspondencia de X en Y. Igual ocurre si nos planteamos la reescritura de la relación inversa de R como correspondencia.

Evitaremos lo anterior adoptando como noción primitiva a la hora de hablar de inversa de una correspondencia la condición de ser ésta una función inyectiva.

Definición 12.6.— Si una función $f : X \longrightarrow Y$ es inyectiva, hablamos de $f^{-1} : Y \longrightarrow X$, que asocia a y el único x tal que $f(x) = y$, y denominamos función *inversa* (o *recíproca*) de f y también es inyectiva (por ser f una función).

Dicho de otro modo, si f es inyectiva y viene dada por la terna $\langle X, Y, G_f\rangle$, entonces f^{-1} también es inyectiva y viene dada por la terna $\langle X, Y, G_{f^{-1}}\rangle$ donde $G_{f^{-1}} = \{\langle y, x\rangle : \langle x, y\rangle \in G_f\}$.

Teorema 12.4

Sean $f : X \longrightarrow Y$ una función inyectiva y $V, W \subseteq Y$. Se satisface que:

0. $\operatorname{dom} f^{-1} = \operatorname{ran} f$;
1. $\operatorname{ran} f^{-1} = \operatorname{dom} f$;
2. $\operatorname{cam} f^{-1} = \operatorname{cam} f$;
3. f^{-1} es función inyectiva;
4. si f es aplicación, entonces f^{-1} es función sobreyectiva;
5. si f y f^{-1} son aplicaciones, entonces ambas son aplicaciones biyectivas;
6. si f es biyectiva, entonces $f^{-1} \circ f = I_X$ y $f \circ f^{-1} = I_Y$;
7. $(f^{-1})^{-1} = f$;
8. $f^{-1}(V \cup W) = f^{-1}(V) \cup f^{-1}(W)$;
9. $f^{-1}(V \cap W) = f^{-1}(V) \cap f^{-1}(W)$;
10. $f : X \longrightarrow Y$ es biyectiva si, y sólo si, $\exists f^{-1} : Y \longrightarrow X$ y f^{-1} es biyectiva.

Codificación y descodificación

La codificación de un *alfabeto fuente* Σ en un *alfabeto código* T se realiza mediante una aplicación inyectiva $c : \Sigma \longrightarrow T^*$, siendo T^* el conjunto de palabras formadas exclusivamente con letras de T —*cfr. supra* § 7 (pág. lxxxv de esta edición)—. Del rango de c se dice que es un *código* de Σ sobre T y de cada uno de sus elementos que es una *palabra código* (concretamente, una *codificación* de una letra de Σ).

Por ejemplo, una codificación del alfabeto fuente $\Sigma = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ en el alfabeto código $T = \{0, 1\}$ viene dada por la aplicación $c_I : \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \longrightarrow \{0, 1\}$ definida por: $0 \longmapsto 0$, $1 \longmapsto 1$, $2 \longmapsto 10$, $3 \longmapsto 11$, $4 \longmapsto 100$, $5 \longmapsto 101$, $6 \longmapsto 110$, $7 \longmapsto 111$, $8 \longmapsto 1000$, $9 \longmapsto 1001$. Llamemos código C_I a $\operatorname{ran} c_I$. Se trata de un *código binario de longitud variable*. Sin embargo, a veces resultan útiles otras codificaciones binarias. A modo de ejemplo, otra codificación de $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ en $\{0, 1\}$ viene dada por la aplicación $c_{II} : \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\} \longrightarrow \{0, 1\}$ definida por: $0 \longmapsto 00011$, $1 \longmapsto 11000$, $2 \longmapsto 10100$, $3 \longmapsto 01100$, $4 \longmapsto 10010$, $5 \longmapsto 01010$, $6 \longmapsto 00110$, $7 \longmapsto 10001$, $8 \longmapsto 01001$, $9 \longmapsto 00101$. Llamemos código C_{II} a $\operatorname{ran} c_{II}$. Se trata de un *código binario en bloque* de longitud 5. Por cierto, éste es un *código detector de errores*: cada palabra tiene exactamente dos unos y tres ceros y si durante la transmisión de la información un error afectase a un carácter se produciría un cambio de paridad fácilmente detectable —si bien no pudiésemos recuperar la información enviada (no es un *código corrector de errores*)—.

La *codificación de un mensaje* escrito exclusivamente con letras de Σ se realiza mediante la extensión c^* de c al conjunto Σ^*, esto es, mediante la aplicación $c^* : \Sigma^* \longrightarrow T^*$ definida por $c^*(a_{i_0} a_{i_1} \cdots a_{i_n}) = c(a_{i_0}) c(a_{i_1}) \cdots c(a_{i_n})$,

Se dice que un código de Σ^* sobre T^* tiene *descodificación única* precisamente si c^* es inyectiva, en otras palabras, precisamente si existe $(c^*)^{-1} : T^* \longrightarrow \Sigma^*$. Éstos, en principio, son los códigos de interés en la codificación de la información desde el punto de vista de la transmisión de ésta.

En particular, de los dos ejemplos de códigos que hemos puesto, sólo $\mathcal{C}_{II}$ tiene descodificación única. A modo de ejemplo, las codificaciones del mensaje 357 son 11101111 en por $\mathcal{C}_I$ y 011000101010001 por $\mathcal{C}_{II}$. Observamos que 11101111 también es una codificación por $\mathcal{C}_I$ de 7033, es decir, la aplicación c_I no es inyectiva; en otras palabras, $\mathcal{C}_I$ no tiene descodificación única. En el caso de $\mathcal{C}_{II}$, tener longitud fija es determinante para que tenga descodificación única.

Inversión de programas

Tras un ciberataque, ¿no sería genial disponer de una contramedida que dejase todo en el mismo estado que antes? Un posible punto de partida es la inversión de programas. Sea P el programa `x := x + 1`, tras su ejecución, todo volvería a ser como antes si ejecutásemos el que pudiésemos designar por P^{-1} y denominar programa inverso de P, `x := x - 1`. Observemos que en este caso subyacen las funciones $x \longrightarrow x+1$ y su inversa $x \longrightarrow x-1$. Un punto de inicio genial para aprender sobre inversión de programas es [56] (cap. 21, págs. 265–274).

§ 12.4 Función característica de un conjunto

Definición 12.7.— Dados un conjunto de referencia U y un subconjunto suyo, X. Para expresar el hecho de que un elemento x de U pertenezca a X, utilizamos el concepto de *función característica* (o, sinónimamente, *función indicadora, indicatriz, de pertenencia o de membresía*):

$$\begin{array}{rccl} \mu_X : & U & \longrightarrow & \{0,1\} \\ & x & \longmapsto & \mu_X(x) = \begin{cases} 1 & \text{si } x \in X \\ 0 & \text{si } x \notin X \end{cases} \end{array}$$

Es posible caracterizar todo lo estudiado anteriormente en términos de la función característica. Tenemos, por ejemplo, el siguiente teorema.

Teorema 12.5

$\forall X, Y \subseteq U, \forall x \in U$:

0. conjunto de referencia (U):	$\mu_U(x) = 1$;
1. conjunto vacío ($\emptyset$):	$\mu_\emptyset(x) = 0$;
2. inclusión (I) ($X \subseteq U$):	$\mu_X(x) \leq \mu_U(x)$;
3. inclusión (II) ($X \subseteq Y$):	$\mu_X(x) \leq \mu_Y(x)$;
4. complementación ($X^\complement$):	$\mu_{X^\complement}(x) = 1 - \mu_X(x)$;
5. intersección (I) ($X \cap Y$):	$\mu_{X \cap Y}(x) = \mu_X(x) \cdot \mu_Y(x)$;
6. intersección (II) ($X \cap Y$):	$\mu_{X \cap Y}(x) = \min\{\mu_X(x), \mu_Y(x)\}$;
7. unión (I) ($X \cup Y$):	$\mu_{X \cup Y}(x) = \mu_X(x) + \mu_Y(x) - \mu_{X \cap Y}(x)$;
8. unión (II) ($X \cup Y$):	$\mu_{X \cup Y}(x) = \max\{\mu_X(x), \mu_Y(x)\}$;
9. diferencia ($X \setminus Y$):	$\mu_{X \setminus Y}(x) = \mu_{X \cap Y^\complement}(x)$;
10. diferencia simétrica ($X \Delta Y$):	$\mu_{X \Delta Y}(x) = \mu_{(X \setminus Y) \cup (Y \setminus X)}(x)$;
11. idempotencia:	$\mu_X^2(x) = \mu_X(x)$.

Observación 12.4.0.— Es posible:

- redefinir la unión en función de la suma algebraica, $A \dotplus B$: $\mu_{A \dotplus B} = \mu_A(x) + \mu_B(x) \cdot \mu_{A \cdot B}$, que llamamos *suma de* Boole (o, sinónimamente, *suma booleana*), siendo de interés por ejemplo, para la teoría de los conjuntos borrosos (*fuzzy sets*) —generalización de la teoría de los conjuntos ordinarios (aunque en ese entorno hablamos de *suma algebraica*)—, y
- redefinir la intersección en función del producto algebraico, $A \cdot B$: $\mu_{A \cdot B} = \mu_A(x) \cdot \mu_B(x)$, que llamamos *producto de* Boole (o, sinónimamente, *producto booleano*), siendo también de interés para la teoría de los conjuntos borrosos, aunque en ese entorno hablamos de *producto algebraico*.

Ejemplo 365

Demostremos los apartados 3, 4, 6, 7 y 11 del teorema 12.5 (pág. 699 de esta edición).

Resolución.— En efecto:

3. $Y = (X \cap Y) \cup (X^\complement \cap Y), x \in X \cap Y \leftrightarrow \mu_X(x) = \mu_Y(x) = 1, x \in X^\complement \cap Y \leftrightarrow \mu_X(x) = 0 < 1 = \mu_Y(x)$;

4. si $x \in X^\complement$, entonces $\mu_{X^\complement}(x) = 1 = 1 - 0 = 1 - \mu_X(x)$; si $x \notin X^\complement$, entonces $\mu_{X^\complement}(x) = 0 = 1 - 1 = 1 - \mu_X(x)$;

6. $\mu_{X\cap Y}(x) = 1$ si, y sólo si, $x \in X \cap Y$ si, y sólo si, $x \in X$ y $x \in Y$ si, y sólo si, $\mu_X(x) = 1$ y $\mu_Y(x) = 1$ si, y sólo si $\min\{\mu_X(x), \mu_Y(x)\} = 1$.

7. $\mu_{X\cup Y}(x) = 1-\mu_{(X\cup Y)^{\complement}}(x) = 1-\mu_{X^{\complement}\cap Y^{\complement}}(x) = 1-\mu_{X^{\complement}}(x)\cdot\mu_{Y^{\complement}}(x) = 1-(1-\mu_X(x))\cdot(1-\mu_Y(x)) = \mu_X(x)+\mu_Y(x)-\mu_X(x)\cdot\mu_Y(x) = \mu_X(x)+\mu_Y(x)-\mu_{X\cap Y}(x)$;

11. $\mu_X^2(x) = \mu_X(x)\cdot\mu_X(x) = \mu_{X\cap X}(x) = \mu_X(x)$. ■

Teorema 12.6 (Principio de inclusión-exclusión)
Dados X, Y y Z, conjuntos, se satisface:

0. $\mu_{X\cup Y} = \mu_X + \mu_Y - \mu_{X\cap Y}$ (apartado 7 del teorema 12.5 [pág. 699 de esta edición]);
1. $\mu_{X\cup Y\cup Z} = \mu_X + \mu_Y + \mu_Z - \mu_{X\cap Y} - \mu_{X\cap Z} - \mu_{Y\cap Z} + \mu_{X\cap Y\cap Z}$;
2. $\mu_{\bigcup_{i=0}^{n} X_i} = \sum_{i=0}^{n}\mu_{X_i} - \sum_{\substack{i,j\in\{0,1,\dots,n\}\\ i<j}}\mu_{X_i\cap X_j} + \cdots + (-1)^n\mu_{X_0\cap X_1\cap\dots\cap X_n}$.

Observación 12.4.1.— Una relación diádica no es más que un grafo (en el sentido de Berge), $G \subseteq E_0 \times E_1$, tal que $\forall(x,y) \in E_0 \times E_1$, $\mu_G(x,y) \in \{0,1\}$, de manera que $xGy \leftrightarrow \mu_G(x,y) = 1$. Igualmente es posible expresar en términos de la función característica todas las propiedades y resultados estudiados para relaciones.

§ 12.5 Órdenes y aplicaciones

Definición 12.8.— Sean $(X, \preccurlyeq_1)$ y $(Y, \preccurlyeq_2)$ dos conjuntos ordenados y $f : X \longrightarrow Y$ una aplicación . Decimos que:

0. f es *creciente* $\leftrightharpoons (\forall x, y \in X)(x \preccurlyeq_1 y \rightarrow f(x) \preccurlyeq_2 f(y))$;

1. f es *decreciente* $\leftrightharpoons (\forall x, y \in X)(x \preccurlyeq_1 y \rightarrow f(y) \preccurlyeq_2 f(x))$;

2. f es *monótona* $\leftrightharpoons$ f es creciente o decreciente;

3. f es *estricta creciente* $\leftrightharpoons (\forall x, y \in X)(x \prec_1 y \rightarrow f(x) \prec_1 f(y))$;

4. f es *estricta decreciente* $\leftrightharpoons (\forall x, y \in X)(x \prec_1 y \rightarrow f(y) \prec_2 f(x))$;

5. f es *estricta monótona* $\leftrightharpoons$ f es estricta creciente o estricta decreciente;

6. f es *isomorfismo de orden* (o, sinónimamente, *isomorfismo entre conjuntos ordenados* o *isomorfismo isótono*) $\leftrightharpoons$ f es biyectiva y $(\forall x, y \in X)(x \preccurlyeq_1 y \leftrightarrow f(x) \preccurlyeq_2 f(y))$.

Teorema 12.7
Sean $(X, \preccurlyeq_1)$ un conjunto totalmente ordenado, $(Y, \preccurlyeq_2)$ un conjunto parcialmente ordenado y $f : X \longrightarrow Y$ una aplicación, entonces:

0. si f es estricta monótona, entonces f es inyectiva;
1. si f es estricta creciente, entonces f es isomorfismo entre X y $f(X)$.

Definición 12.9.— Sea $(X; \preccurlyeq)$ un conjunto ordenado y $f : X \longrightarrow X$ una aplicación. Decimos que:

0. f es *extensiva* $\leftrightharpoons (\forall x \in X)(x \preccurlyeq f(x))$;
1. f es *idempotente* $\leftrightharpoons (\forall x \in X)(f(f(x)) = f(x))$;
2. f es *de cierre* $\leftrightharpoons$ si f es creciente, extensiva e idempotente.

§ 12.6 Operación en un conjunto

Una *operación* es un proceso aplicado a uno o más objetos denominados *operandos* o *argumentos* mediante el que se obtiene un resultado. Generalmente una operación se escribe con un símbolo específico llamado *operador*. Si tiene dos operandos, se trata de una operación *diádica* (o, sinónimamente, *binaria*), si tiene tres, una operación *triádica* (o, sinónimamente, *ternaria*), si cuatro, *tetrádica* (o, sinónimamente, *cuaternaria*), si cinco, *pentádica* (o, sinónimamente, *quinaria*), etc.

Dado un conjunto $X \neq \emptyset$ y una operación $*$ entre los elementos de X, decimos que

- la operación $*$ es *siempre posible* en X precisamente si el resultado es un elemento de X, es decir, en el caso de que sean dos los operandos de $*$ esto equivale a que $\forall x, y \in X, \exists z \in X$ tal que $x * y = z$;
- la operación $*$ es *uniforme* en X precisamente si ocurre que si el resultado es un elemento de X entonces es único, es decir, en el caso de que sean dos los operandos de $*$ esto equivale a que $\forall x, y \in X$, si existe $z \in X$ tal que $x * y = z$, entonces z es único.

Definición 12.10.— Llamamos *ley de composición interna (l.c.i)* (o, sinónimamente, *operación interna*) en X a cualquier operación siempre posible y uniforme en X, lo que es tanto como decir que es una aplicación.

Definición 12.11.— Llamamos *ley de composición externa* (l.c.e.) en X a toda aplicación $f : S \times X \longrightarrow X, \langle \alpha, x \rangle \longmapsto f(\alpha, x)$, siendo habitual notar $f(\alpha, x)$ simplemente por αx (suele llamarse conjunto de escalares a S)[1].

[1] En estas notas sólo mencionamos las l.c.e. en ciertas definiciones, por ejemplo, en la de espacio vectorial (*cfr. infra* definición 17.96 [pág. 927 de esta edición]).

Ejemplo 366

¿Qué significa en la definición anterior que sea «tanto como decir que es una aplicación»?

Resolución.— Pues que, por ejemplo, en el caso de que sean dos los operandos de $*$, decir que $*$ es una l.c.i. en X es tanto como decir que $* : X \times X \longrightarrow X$ es una aplicación, en definitiva, una relación triádica homogénea —*vid. supra* definición 11.0 (pág. 601 de esta edición)— y funcional (o sea, un subconjunto de $(X \times X) \times X)$ cuyo dominio es $X \times X$. ■

ⓘ De aquí en adelante, entendemos por *operación* una operación interna.

Definición 12.12.— Dados un conjunto $X \neq \emptyset$ y $* : X \times X \longrightarrow X$ una operación diádica en X, son frecuentes tres notaciones para el resultado de operar dos elementos $x, y \in X$:

- *prefijo*: $*xy$, o bien, $*(x, y)$;
- *infijo*: $x * y$;
- *sufijo* (o, sinónimamente, *postfijo*): $xy*$, o bien, $(x, y)*$.

Para el caso de una operación enádica $* : X^n \longrightarrow X$ y n elementos de X, $x_0, x_1, \ldots, x_{n-1}$, es similar: *prefijo*: $*x_0x_1 \ldots x_{n-1}$, o bien, $*(x_0, x_1, \ldots, x_{n-1})$, *infijo*: $x_0 * x_1 * \cdots * x_{n-1}$ y *postfijo*: $x_0x_1 \ldots x_{n-1}*$, o bien, $(x_0, x_1, \ldots, x_{n-1})*$.

Definición 12.13.— Dados un conjunto $X \neq \emptyset$ y $* : X^n \longrightarrow X$ una operación enádica en X, decimos que un subconjunto $Y \subseteq X$ es *parte estable* de $(X; *)$ (o, sinónimamente, que Y es *cerrado* para $*$) precisamente si:

$$(\forall x_0, x_1, \ldots, x_{n-1} \in Y)\,(x_0 * x_1 * \cdots * x_{n-1} \in Y)$$

Definición 12.14.— Sean un conjunto $X \neq \emptyset$ y $* : X \times X \longrightarrow X$ una operación diádica en X. Sean $x, y \in X$. Decimos que:

- x y y son *elementos permutables*, en X para $*$ (o, sinónimamente, que x permuta con y, o viceversa) precisamente si $x * y = y * x$;
- x es un *elemento central* en X para $*$ precisamente si permuta con todo elemento de X;
- el *centro* de X para $*$ es el conjunto de todos los elementos centrales de X.

Definición 12.15.— Sean un conjunto $X \neq \emptyset$ y $* : X \times X \longrightarrow X$ una operación diádica en X. Decimos que $*$ es *conmutativa* en X precisamente si el centro de X es X, esto es, si, y sólo si, $\forall x, y \in X$,

$$x * y = y * x.$$

Definición 12.16.— Sean un conjunto $X \neq \emptyset$ y $* : X \times X \longrightarrow X$ una operación diádica en X. Decimos que $*$ es *asociativa* en X precisamente si $\forall x, y, z \in X$,

$$(x * y) * z = x * (y * z).$$

Ejemplo 367

Razonemos que cualquier juntor es una operación en el conjunto de todas las fórmulas de la lógica de juntores.

Resolución.— En efecto, el negador es una operación monádica, $\neg : \mathcal{F}_0 \longrightarrow \mathcal{F}_0$ y los juntores diádicos son operaciones diádicas de $\mathcal{F}_0 \times \mathcal{F}_0$ en $\mathcal{F}_0$. A modo de ejemplo, la disyunción, la conjunción, la disyunción exclusiva y el bicondicional son operaciones conmutativas y asociativas, mientras que el condicional es una operación no conmutativa ni asociativa. ■

Ejemplo 368

Analicemos las aplicaciones $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ (suma de números enteros) y $- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ (diferencia de números enteros) como operaciones en $\mathbb{Z}$.

Resolución.— Veamos:

0. $+$ y $-$ son operaciones diádicas sobre $\mathbb{Z}$;
1. su notación es infija;
2. $\mathbb{N}$ es parte estable para $+$ pero no lo es para $-$; en efecto, $\exists x, y \in \mathbb{N}, x - y \notin \mathbb{N}$, por ejemplo, $x = 3, y = 7$;
3. $\mathbb{Z}$ es parte estable para $+$ y para $-$;
4. cualesquiera dos números naturales o dos números enteros son permutables para $+$;
5. justamente por el punto anterior (4), el centro de $\mathbb{N}$ para $+$ es $\mathbb{N}$ y el centro de $\mathbb{Z}$ para $+$ es $\mathbb{Z}$, en otras palabras, $+$ es conmutativa en $\mathbb{N}$ y en $\mathbb{Z}$; sin embargo, no existen elementos centrales para $-$, ni en $\mathbb{N}$ ni en $\mathbb{Z}$, en otras palabras, el centro de $\mathbb{N}$ y de $\mathbb{Z}$ para $-$ es $\emptyset$;
6. $+$ es asociativa en $\mathbb{N}$ y en $\mathbb{Z}$;

7. $-$ no es asociativa en $\mathbb{N}$ y, por tanto, tampoco en $\mathbb{Z}$; por ejemplo, $(0-1)-2=-1-2=-3 \neq 1=0-(-1)=0-(1-2)$. ■

Una operación $*$ en un conjunto $\{\dots, a_i, \dots, a_j, \dots\}$ puede representarse por una tabla de doble entrada, la *tabla de composición* (o, sinónimamente, *tabla de* CAYLEY) de la operación, donde cada celda se interpreta de la forma

$*$	$\dots$	a_j	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
a_i	$\dots$	$a_i * a_j$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Por ejemplo, la operación producto en el conjunto $\{0, 1\}$,

$\cdot$	0	1
0	0	0
1	0	1

Ejemplo 369

¿Puede ser una colección de conjuntos cerrada para las operaciones diádicas unión finita e intersección finita y no serlo para la operación monádica complementación?

Resolución.— Sí, sea el intervalo entero abierto $\{x \in \mathbb{Z} : n < x\}$, que abreviamos por (n, ∞), y consideremos la colección de todos ellos, $\mathcal{A} = \{(n, \infty) : n \in \mathbb{Z}\}$. Claramente, $\mathcal{A}$ es cerrada para la unión y la intersección finita:

$$(m, \infty) \cup (n, \infty) = (\min\{m, n\}, \infty),$$
$$(m, \infty) \cap (n, \infty) = (\max\{m, n\}, \infty).$$

Sin embargo, no lo es para la complementación:

$$(n, \infty)^{\complement} = (-\infty, n] \notin \mathcal{A}.$$ ■

Actividad 12.0

Conozcamos la *sucesión de hiperoperaciones*. Una referencia pudiese ser el artículo Hiperoperación (https://es.wikipedia.org/wiki/Hiperoperación).

§ 12.7 Multiconjuntos

En principio, dado un conjunto X, un multiconjunto es cualquier disposición no ordenada y con repetición de elementos de X.

No existe una notación estándar; dos entre las más frecuentes son las dobles llaves $\{\{\}\}$ y las llaves recíprocas $\}\{$, ambas por extensión, con todos los elementos y sus repeticiones.

Ejemplo 370

Interpretemos el conjunto de pares ordenados $\{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \dots\}$ como un multiconjunto.

Resolución.— Interpretando que las primeras componentes de los pares designan números naturales y las segundas el número de veces que se repite el número natural de sus correspondientes primeras (su multiplicidad), entonces $\{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \dots\}$ designa el multiconjunto $\{\{1,2,2,3,3,3,\dots\}\}$. ∎

Definición 12.17.— Sea S un conjunto finito. Un *multiconjunto* (o, sinónimamente, *mconjunto*, brevemente) formado por elementos de S es un par (X,m), con $X \subseteq S$ y $m : X \longrightarrow \mathbb{Z}^+$ la aplicación que asigna a cada $x \in X$ su multiplicidad $m(x)$, esto es, el número de veces que aparece repetido en el multiconjunto.

Observación 12.7.0.— Un ejemplo de una tercera notación es $[x_0, x_1, \dots, x_n]_{m_0, m_1, \dots, m_n}$, donde m_i abrevia $m(x_i)$ ($0 \leq i < n+1$); por ejemplo, $[a,b,c]_{1,2,3}$ designa el multiconjunto $\{\{a,b,b,c,c,c\}\}$ y $[1,2,3,\dots]_{1,2,3,\dots}$ designa el multiconjunto $\{\{1,2,2,3,3,3,\dots\}\}$ —esta notación aparece, por ejemplo, en Blizard [178]—.

Definición 12.18.— Siendo (X,m) un multiconjunto, decimos que X es su *conjunto subyacente* (o, sinónimamente, *conjunto soporte*).

Definición 12.19.— La *cardinalidad* (o, sinónimamente, *cardinal*) de un multiconjunto es la suma de todas las multiplicidades de los elementos de su conjunto subyacente, en otras palabras,

$$|(X,m)| = \sum_{x \in X} m(x).$$

Definición 12.20.— Dado (X,m), $Y \subseteq X$ y $m' : Y \longrightarrow \mathbb{Z}^+$, con $m'(y) \leq m(y)$, para todo $y \in Y$, decimos que (Y,m') es un *submulticonjunto* del multiconjunto (X,m) (de éste en relación con aquél, decimos que es un supermulticonjunto suyo).

En adelante, $(M_k((X, m))$ designa el conjunto de todos los submulticonjuntos de (X, m) de cardinalidad k.

Observación 12.7.1.— Anticipamos que si $|X| = n$, entonces

$$|(M_k((X, m))| = CR(n, k),$$

las combinaciones con repetición de n elementos tomados de k en k.[2]

Para los multiconjuntos elegimos como notación de su representación por extensión las dobles llaves, por ejemplo, si $S = \{x, y, z\}$, $X = \{x, y\}$ y $m : X \longrightarrow \mathbb{Z}^+$ se define por $m(x) = 2$ y $m(y) = 3$, entonces (X, m) es $\{\{x, x, y, y, y\}\}$ —y, ocasionalmente, la de la observación 12.7.0 (pág. 705 de esta edición), en este caso, $[x, y]_{2,3}$—.

§ 12.8 Continuidad discreta

Como afirma Johnsonbaugh [179], son muchos los resultados que nos ofrece la matemática en sus versiones discreta y continua. Veamos a continuación, un versión discreta de la continuidad y las versiones discretas del teorema de Bolzano y del teorema del valor intermedio.

No existe una notación estándar para un *intervalo numérico discreto*; en la literatura encontramos varias designaciones para el conjunto de números enteros $\{z \in \mathbb{Z} : x \leq z < y\}$, por ejemplo, $[x, y) \cap \mathbb{Z}$, $[x, y)_{\mathbb{Z}}$ o $[\![x, y)\!)$. Optamos por la última, si bien a veces usaremos la penúltima.

Definición 12.21.— Dados $x, y \in \mathbb{Z}$, definimos:

- $[\![x, y]\!] = \{z \in \mathbb{Z} : x \leq z \leq y\}$, *intervalo entero cerrado* de extremo inferior x y extremo superior y;
- $(\!(x, y)\!) = \{z \in \mathbb{Z} : x < z < y\}$, *intervalo entero abierto* de extremo inferior x y extremo superior y;
- $[\![x, y)\!) = \{z \in \mathbb{Z} : x \leq z < y\}$, *intervalo entero abierto por la izquierda y cerrado por la derecha*, de extremo inferior x y extremo superior y;
- $(\!(x, y]\!] = \{z \in \mathbb{Z} : x < z \leq y\}$, *intervalo entero cerrado por la izquierda y abierto por la derecha*, de extremo inferior x y extremo superior y;
- $(\!(x, +\infty)\!) = \{z \in \mathbb{Z} : x < z\}$, *intervalo entero abierto no acotado por la derecha*, de extremo inferior x;

[2] *Cfr. infra* definición 19.39 (pág. 1180 de esta edición).

- $[\![x, +\infty)\!) = \{z \in \mathbb{Z} : x \leq z\}$, *intervalo entero cerrado no acotado por la derecha*, de extremo inferior x;
- $(\!(-\infty, y)\!) = \{z \in \mathbb{Z} : z < y\}$, *intervalo entero abierto no acotado por la izquierda*, de extremo superior y;
- $(\!(-\infty, y]\!] = \{z \in \mathbb{Z} : z \leq y\}$, *intervalo entero cerrado no acotado por la izquierda*, de extremo superior y;
- $(\!(-\infty, +\infty)\!) = \mathbb{Z}$.

Definición 12.22.— Sean $m, n \in \mathbb{Z}$, $m < n$ y $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ una aplicación. Decimos que f es una *aplicación discretamente continua* en $[\![m, n]\!]$ precisamente si para cualquier entero i, $m \leq i < n$, la distancia entre $f(i)$ y $f(i+1)$ es como mucho 1, es decir, si, y sólo si, $\forall i \in [\![m, n)\!)$, $|f(i) - f(i+1)| \leq 1$.

La versión discreta del teorema de BOLZANO es la siguiente.

Teorema 12.8 (Teorema de BOLZANO, discreto)
Sea $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ una aplicación discretamente continua en $[\![m, n]\!]$ y tal que $f(m)f(n) < 0$, entonces $\exists x \in (\!(m, n)\!)$ tal que $f(x) = 0$.

Demostración.— Sean $S \coloneqq \{x \in [\![m, n]\!] : f(x) > 0\}$ y $s \coloneqq \max S + 1$; veamos que $f(s) = 0$. Demostrémoslo por contraposición. Supongamos lo contrario, o sea, que $f(s) < 0$ o $f(s) > 0$, entonces, por un lado, de ser $f(s) < 0$, se tendría que $s \in S$ (por definición de S), lo que contradiría que $s - 1$ es una cota superior de S y, por otro, de ser $f(s) > 0$, se tendría que $f(s-1) \geq 0$ (por ser f discretamente continua), entonces $s - 1 = \max S \notin S$. ∎

La versión discreta del teorema del valor intermedio es la siguiente.

Teorema 12.9 (Teorema del valor intermedio, discreto)
Sea $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ una aplicación discretamente continua en $[\![m, n]\!]$, entonces para cualquier $y \in \mathbb{Z}$ tal que $\min\{f(m), f(n)\} < y < \max\{f(m), f(n)\}$, $\exists x \in (\!(m, n)\!)$ tal que $f(x) = y$.

Demostración.— Sin pérdida de generalidad, supongamos que $f(m) < f(n)$. Sea $g : \mathbb{Z} \mapsto \mathbb{Z}$ definida por $g(x) = f(x) - y$; g es discretamente continua en $[\![m, n]\!]$ por serlo f, $g(m) < 0$ por ser $f(m) < y$ y $g(n) > 0$ por ser $f(n) > 0$; por tanto, por el teorema de BOLZANO discreto, $\exists x \in (\!(m, n)\!)$ tal que $g(x) = 0$, o sea, $f(x) = y$. ∎

Por cierto, el número de enteros en el intervalo real $(x, y]$ es $\lfloor y \rfloor - \lfloor x \rfloor$.

Ejemplo 371

Basándonos en el ejemplo que propone JOHNSONBAUGH [179], veamos el siguiente —por cierto, ¿nos acordamos del sistema formal MIU (*cfr. supra* ejemplo 119 (pág. 185 de esta edición)?, porque tiene un cierto aire familiar, ¿verdad?—. Sea B el conjunto de todas las palabras binarias generadas a partir de la palabra vacía mediante las tres reglas de producción siguientes (α y β son dos palabras cualesquiera de B):

$$R_0 : \frac{\alpha}{0\alpha 1} \quad R_1 : \frac{\alpha}{1\alpha 0} \quad R_2 : \frac{\alpha \quad \beta}{\alpha\beta}$$

Por definición de B, todas las palabras generadas tienen el mismo número de ceros que de unos. Demostremos que el recíproco también es cierto, es decir, que si una palabra binaria tiene el mismo número de ceros que de unos, entonces es un elemento de B.

Resolución.— Notemos por $\mathrm{N}(c, x)$ el número de apariciones de x en la palabra c. Sea b una palabra binaria con el mismo número de ceros que de unos, es decir, tal que $\mathrm{N}(b, 0) = \mathrm{N}(b, 1)$. Vamos a demostrar por inducción fuerte (*cfr.* infra teorema 16.3 [pág. 810 de esta edición]) que $b \in B$. Sea n la longitud de b. Notando «una palabra binaria de longitud n con el mismo número de ceros que de unos está en B» por $P(n)$, lo que nos proponemos es demostrar que $\forall n \in \mathbb{N}, P(n)$. Para ello, apliquemos el teorema 16.3 (pág. 810 de esta edición) (inducción fuerte):

Caso base.— Si $n = 0$, b es la palabra vacía que, por definición de B, está en B, es decir, $P(0)$ es verdadera.

Hipótesis inductiva fuerte.— Siendo $n > 0$, cualquier palabra binaria de longitud $k < n$ con igual número de ceros que de unos está en B, es decir, $P(0) \wedge P(1) \wedge \ldots \wedge P(k)$, para todo $k < n$.

Paso inductivo fuerte.— Supongamos $P(0), P(1), \ldots, P(k)$ y demostremos $P(k+1)$; distingamos tres casos:

I. si b comienza con 0 y termina con 1, o sea, si existe una palabra binaria α tal que $b = 0\alpha 1$, entonces α tiene el mismo número de ceros que de unos (por ocurrir para b) y como $|\alpha| = |b| - 2$, por hipótesis inductiva fuerte $\alpha \in B$, de donde, por la regla R_0, $b \in B$;

II. si b comienza con 1 y termina con 0, entonces por un razonamiento análogo al anterior tenemos, por la regla R_1, que $b \in B$;

III. si b comienza y termina con 0, entonces,

0. sea la aplicación $f : [\![1, n-1]\!] \longrightarrow \mathbb{Z}$, definida por $f(i) = \mathrm{N}(b_{[i]}, 0) - \mathrm{N}(b_{[i]}, 1)$, donde $b_{[i]}$ designa el prefijo de b de longitud i;

1. en particular, tenemos que $f(1) = 1 - 0 = 1 > 0$ (b comienza con 0, luego el prefijo de longitud 1 de b, el primer bit, tiene un 0 y ningún 1) y que $f(n-1) = -1 < 0$ (b

termina en 0 y b tiene igual número de ceros que de unos, luego el prefijo de longitud $n-1$ de b, los $n-1$ primeros bits, tiene un 0 menos);

2. por otro lado, por definición, $f(i)$ y $f(i+1)$ difieren en 1, sea cual sea $i \in [\![1, n-1]\!]$, por lo que f es discretamente continua en $[\![1, n-1]\!]$;

3. por tanto, aplicando el teorema de Bolzano discreto a f en $[\![1, n-1]\!]$, se sigue que $\exists i \in (\!|1, n-1|\!)$ tal que $f(i) = 0$, en otras palabras que existe un prefijo de b, digamos α, de longitud i mayor que 1 y menor que $n-1$ que tiene el mismo número de ceros que de unos, por lo que por hipótesis inductiva, $\alpha \in B$;

4. la existencia de α implica que el sufijo de b, digamos β, de longitud $n-i$, complementario de α también tiene el mismo número de ceros que de unos y también su longitud es menor que n y, por tanto, por hipótesis inductiva, $\beta \in B$;

5. por la regla R_2, la concatenación de ambas, $\alpha\beta$, que es precisamente b, está en B;

IV. si b comienza y termina con 1, entonces por un razonamiento análogo al anterior se sigue que $b \in B$.

Conclusión.— Como se satisfacen el caso base y el paso inductivo fuerte, entonces del teorema 16.3 (pág. 810 de esta edición), de inducción fuerte, se sigue lo buscado, a saber, que $\forall n \in \mathbb{N}, P(n)$. ■

§ 12.9 Muestra de más ejemplos

Ejemplo 372

Sean X y Y dos conjuntos cualesquiera, finitos o no, tales que $|X \setminus Y| = |Y \setminus X|$. Demostremos que este hecho implica que $|X| = |Y|$.

[EPF 14.5.2019:4].

Resolución.— La igualdad $|X \setminus Y| = |Y \setminus X|$ equivale a que existe una aplicación biyectiva, digamos g, de $X \setminus Y$ en $Y \setminus X$, que a los elementos x de X que no están en Y, les hace corresponder un elemento $g(x)$ de Y. Esto nos lleva a pensar en definir la correspondencia:

$$f : X \longrightarrow Y$$
$$x \longrightarrow \begin{cases} x & \text{si } x \in Y \\ g(x) & \text{si } x \notin Y \end{cases}$$

Resulta que f es una aplicación biyectiva de $X = (X \cap Y)\dot{\cup}(X \setminus Y)$ en $Y = (X \cap Y)\dot{\cup}(Y \setminus X)$, por serlo x (la aplicación identidad) de $X \cap Y$ en $X \cap Y$ y serlo, por hipótesis, g de $X \setminus Y$ en $Y \setminus X$. ■

Ejemplo 373

Sea C un conjunto y $f : 2^C \longrightarrow \mathbb{N}$ una aplicación tal que $\forall X, Y \in 2^C, f(X \cup Y) = f(X) + f(Y)$ si $X \cap Y = \emptyset$.

0. Demostremos que $f(\emptyset) = 0$.
1. Demostremos que $\forall X, Y \in 2^C, f(X \cup Y) = f(X) + f(Y) - f(X \cap Y)$.
2. Expliquemos razonadamente si una correspondencia *Card* con argumento un conjunto finito y valor el cardinal de éste pudiese ser un caso particular de la aplicación f.

[AIC 10.4.2019:2a] (apág. 0), [AIC 10.4.2019:4b] (apág. 1), [EFE 22.6.2022:2]. *Cfr.* Anzola y Caruncho [140]: ejercicio 3.24 (pág. 60).

Resolución.—

0. *De una manera.*

En efecto, por hipótesis —esto es, de lo que satisface f—, como $X \cap \emptyset = \emptyset$, entonces $f(X \cup \emptyset) = f(X) + f(\emptyset)$ y de aquí, $f(\emptyset) = f(X \cup \emptyset) - f(X) = f(X) - f(X) = 0$.

De otra.

Quizás más simple: $\emptyset \cap \emptyset = \emptyset \rightarrow f(\emptyset \cup \emptyset) = f(\emptyset) + f(\emptyset)$ [por hipótesis] $\rightarrow f(\emptyset) = 2f(\emptyset)$ [$\emptyset \cup \emptyset = \emptyset$ y $f(\emptyset) \in \mathbb{N}$] $\rightarrow f(\emptyset) = 0$ [$f(\emptyset) \in \mathbb{N}$].

1. Para cualesquiera $X, Y \in 2^C$:

0.º Y puede reescribirse como la unión disjunta

$$Y = (Y \setminus X) \,\dot{\cup}\, (X \cap Y),$$

por lo que

$$f(Y) = f(Y \setminus X) + f(X \cap Y); \tag{12.0}$$

1.º por otro lado, $X \cup Y$ puede reescribirse como la unión disjunta

$$X \cup Y = X \,\dot{\cup}\, (Y \setminus X),$$

por lo que, por ser f aplicación (todos y cada uno de los subconjuntos de C tienen una única imagen en $\mathbb{N}$):

$$f(X \cup Y) = f(X) + f(Y \setminus X),$$

por lo que

$$f(X) = f(X \cup Y) - f(Y \setminus X); \tag{12.1}$$

2.º finalmente, sumando miembro a miembro (12.0) y (12.1), se tiene

$$\begin{aligned} f(X) + f(Y) &= f(X \cup Y) - f(Y \setminus X) + f(Y \setminus X) + f(X \cap Y) \\ &= f(X \cup Y) + f(X \cap Y), \end{aligned}$$

de donde,

$$f(X \cup Y) = f(X) + f(Y) - f(X \cap Y).$$

2. Si $f(C) = n \in \mathbb{N}$, entonces $(\forall S \subseteq C)(f(S) + f(S^{\complement}) = n)$ [pues $S \cap S^{\complement} = \emptyset$, por lo que, por hipótesis, $f(S) + f(S^{\complement}) = f(S \cup S^{\complement}) = f(C)$]. Si $C = \{1, 2\}$, pudiésemos pensar que $f(C) = 2$ y $f(\{1\}) = f(\{2\}) = 1$, claro que en realidad pueden suceder un número infinito de posibilidades, por ejemplo, que $f(\{1\}) = 1$, $f(\{2\}) = 2$ y $f(\{1, 2\}) = 3$. En definitiva, la respuesta es sí, una correspondencia *Card* con argumento un conjunto finito y valor el cardinal de éste no se identifica con f, pero sí es un caso particular suyo, pues satisface la hipótesis, dado C un conjunto, $Card : 2^C \longrightarrow \mathbb{N}$ es una aplicación tal que $\forall X, Y \in 2^C$, si $X \cap Y = \emptyset$, entonces $Card(X \cup Y) = Card(X) + Card(Y)$; así, por ejemplo, $f(\{1, 2\}) = f(\{1\} \cup \{2\}) = f(\{1\}) + f(\{2\}) = 1 + 1 = 2$, $f(\{1, 2, 3\}) = f(\{1, 2\} \cup \{3\}) = f(\{1, 2\}) + f(\{3\}) = 2 + 1 = 3$, etc.; por otra parte, en la propiedad demostrada en a.2) reconocemos el principio de inclusión-exclusión[3]: $\forall X, Y \in 2^C$, $Card(X \cup Y) = Card(X) + Card(Y) - Card(X \cap Y)$. ■

§ 12.10 Propuesta de más actividades

Actividad 12.1

Sea $A \neq \emptyset$. Decimos que una aplicación $f : A \longrightarrow A$ es una *involución* precisamente si $f \circ f$ es la identidad en A. Sean $a, b \in \mathbb{R}$. Entre las aplicaciones $f : \mathbb{R} \longrightarrow \mathbb{R}$, definidas por $f(x) = ax + b$, encontremos las que son involuciones.

Actividad 12.2

Sean las aplicaciones $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, definida por $f(x, y) = x - y$, y $g : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$, definida por $g(x) = (x, -x)$.

0. Demostremos que f es sobreyectiva y g es inyectiva.
1. ¿Es $f \circ g$ inyectiva? ¿Es $f \circ g$ sobreyectiva?
2. ¿Es $g \circ f$ inyectiva? ¿Es $g \circ f$ sobreyectiva?

[3] *Cfr. infra* teorema 19.27 (pág. 1147 de esta edición).

Actividad 12.3

Sean $A = \{1, 2, 3, 4\}$, $B = \{1, 2\}$ y $f : 2^A \longrightarrow 2^A$, tal que $\forall X \in 2^A$, $f(X) = X \setminus B$.

0. Demostremos que f es una aplicación.
1. Demostremos que $\forall X, Y \in 2^A$, $f(X \cup Y) = f(X) \cup f(Y)$.
2. Demostremos que $\forall X, Y \in 2^A$, $f(X \cap Y) = f(X) \cap f(Y)$.
3. ¿Es f inyectiva?
4. ¿Es f sobreyectiva?

Actividad 12.4

Clasifiquemos (aplicación inyectiva, sobreyectiva o biyectiva) la correspondencia $f : \mathbb{N} \longrightarrow \mathbb{Z}$, definida por: $f(n) = \frac{n}{2}$, si n es par y $f(n) = 3n + 1$, si n es impar.

[Cubit 69], [SEL 4:4].

Actividad 12.5

Clasifiquemos (aplicación inyectiva, sobreyectiva o biyectiva) la correspondencia $f : \mathbb{N} \longrightarrow \mathbb{Z}$, definida por: $f(n) = \frac{n}{2}$, si n es par y $f(n) = -\frac{n+1}{2}$, si n es impar.

[SEL 4:5].

Actividad 12.6

Sean X, Y y Z tres conjuntos y $f : X \longrightarrow Y$ y $g : Y \longrightarrow Z$ dos aplicaciones. Demostremos que:

0. si f y g son inyectivas, entonces $g \circ f$ es inyectiva;
1. si f y g son sobreyectivas, entonces $g \circ f$ es sobreyectiva;
2. si f y g son biyectivas, entonces $g \circ f$ es biyectiva.

[SEL 4:6]. *Cfr.* Anzola y Caruncho [140]: ejercicio 3.25 (pág. 60).

Actividad 12.7

Sea $S_3 = \{0, 1, 2\}$.

0. ¿Cuántas aplicaciones biyectivas hay de S_3 en sí mismo?
1. Representemos dichas biyecciones usando diagrama cartesiano, sagital, matricial y como digrafo.
2. ¿Cuáles son las aplicaciones inversas de cuáles?

[Cubit 72].

Actividad 12.8

Dadas tres funciones f, g y h, decimos que g es una *inversa por la izquierda* de f si $g \circ f = \mathrm{id}_{\mathrm{dom}\, f}$ y que h es una *inversa por la derecha* de f si $f \circ h = \mathrm{id}_{\mathrm{ran}\, f}$. Sean $f : \{0\} \longrightarrow \{1, 2\}$, definida por $f(0) = 1$ y $g : \{1, 2\} \longrightarrow \{0\}$, definida por $g(1) = 0$, $g(2) = 0$. Demostremos que:

0. f es una aplicación inyectiva y no sobreyectiva;
1. g es una aplicación sobreyectiva y no inyectiva;
2. g es una inversa por la izquierda de f;
3. f es una inversa por la derecha de g.

Cfr. TRUSS [141]: §2.2: *Functions*, ejercicio 17 (pág. 78).

§ 12.11 Bibliografía

- Para una primera aproximación:

[145] José GARCÍA GARCÍA y Manuel LÓPEZ PELLICER. *Álgebra lineal y geometría: curso teórico-práctico*. Marfil, Alcoy, Hoya de Alcoy, Alicante (ES-A), España, 8.ª ed., 1992.

[146] Armando Óscar ROJO. *Álgebra I*. El Ateneo, Buenos Aires (AR-C), Argentina, 1986. ©TDR.

- Para estudiar, practicar y saber más:

[140] Máximo ANZOLA GONZÁLEZ y José Ramón CARUNCHO CASTRO. *Problemas de álgebra. Tomo 1: Conjuntos - Grupos*. Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1981. ©TDR.

[144] Agustín de la VILLA CUENCA. *Problemas de Álgebra (con esquemas teóricos)*. CLAGSA, Madrid, Comunidad de Madrid (ES-M), España, 4.ª ed., 2010. ©TDR.

[147] Herbert Bruce ENDERTON. *Elements of Set Theory*. Academic Press, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1977.

[148] Karel HRBACEK y Thomas J. JECH. *Introduction to set theory*. Monographs and textbooks in pure and applied mathematics. Marcel Dekker, Nueva York, Nueva York (US-NY), Estados Unidos de América, 3.ª ed., 1999.

[149] Józef Maria BOCHEŃSKI. *Compendio de lógica matemática*. Colección Lógica y Teoría de la Ciencia. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1982. Traducido del inglés *A Précis of Mathematical Logic* (1959), traducido a su vez de *Précis de logique mathématique* (1948), Bussum, North Holland: F. G. Kroonder.

- Para profundizar, acullá:

[142] José Antonio ALONSO JIMÉNEZ, Joaquín BORREGO DÍAZ, Mario de Jesús PÉREZ JIMÉNEZ y José Luis RUIZ REINA. *Curso Práctico de Teoría de Conjuntos*. La Ñ, Sevilla, Andalucía (ES-AN), España, 1998.

- Sin olvidar a los recomendados dedicados a la matemática discreta:

[32] Félix GARCÍA MERAYO. *Matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 2015.

[141] John Kenneth TRUSS. *Discrete mathematics for computer scientists*. Addison-Wesley, Bungay, Suffolk (GB-SFK), Reino Unido, 1991.

[150] Félix GARCÍA MERAYO, Gregorio HERNÁNDEZ PEÑALVER y Antonio NEVOT LUNA. *Problemas resueltos de matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 2018.

[151] Kenneth Howard ROSEN. *Matemática discreta y sus aplicaciones*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 5.ª ed., 2004. (La 5.ª edición es la última en español).

[152] Kenneth Howard ROSEN. *Discrete Mathematics and its Applications*. McGraw-Hill, Nueva York, Nueva York (US-NY), Estados Unidos de América, 7.ª ed., 2012.

[153] Francisco José GONZÁLEZ GUTIÉRREZ. *Apuntes de Matemática Discreta*. El autor, Cádiz, Andalucía (ES-AN), España, 2004.

[154] Carlos GARCÍA GÓMEZ, Josep María LÓPEZ BESORA y Dolors PUIGJANER RIBA. *Matemática discreta*. Pearson Educación, Madrid, Comunidad de Madrid (ES-M), España, 2002.

[155] Ralph Peter GRIMALDI. *Matemáticas discreta y combinatoria*. Addison-Wesley Iberoamericana, Wilmington, New Castle, Delaware (US-DE), Estados Unidos de América, 3.ª ed., 1997.

[124] Jiří MATOUŠEK y Jaroslav NEŠETŘIL. *Invitación a la matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2008.

[156] Juan Carlos FERRANDO PÉREZ y Valentín GREGORI GREGORI. *Matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2.ª ed., 2012.

[157] Kenneth Allen ROSS y Charles Richard Bowers WRIGHT. *Matemáticas discretas*. Prentice-Hall Hispanoamericana, Naucalpan de Juárez, Estado Libre y Soberano de México (MX-MEX), Estados Unidos Mexicanos, 2.ª ed., 1990.

[158] Richard JOHNSONBAUGH. *Discrete Mathematics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 8.ª ed., 2018.

Capítulo 13

Lógica de lo infinito

Un tiempo tras otro viene.

(Refrán).

El objetivo principal de este capítulo es captar la idea de lo infinito y empezar a conocer cómo manejarla en la matemática y en la computación. La cuestión en el aire es: ¿cuántas veces ha soñado el ser humano con una fuente inagotable en un tiempo inconsumible?

§ 13.0 Tipo de aplicación y cardinal

David HILBERT relata la historia de un hotel con infinitas habitaciones, que según Martin GARDNER populariza, «se extienden hasta un espacio de dimensión superior a través de un agujero negro», numeradas de 1 en adelante. Un buen día, y aunque todo estaba ocupado, se pudo dar cabida a una persona que quería hospedarse, simplemente desplazando a quienes ocupaban cada habitación a la siguiente en número; en otra ocasión, pudo hacerse con cinco personas, sólo se tuvo que desplazar a quienes ocupaban la habitación n a la $n+5$ —para cualquier número de habitación n—. Algo más formalmente, esto corresponde la acción de la aplicación $f : H \longrightarrow H$, definida por $f(h_i) = h_{i+5}$, siendo H el conjunto de todas las habitaciones, con lo que, las 5 primeras habitaciones quedan libres, pues quien ocupa la habitación uno, pasa a alojarse en la habitación $1+5$, etc. Otro día se generó un problema, aparentemente mucho más complicado, llegaron infinitas personas con la pretensión de alojarse; pero también se consiguió, ¿cómo?[o]

Notemos que f y g son aplicaciones inyectivas y no sobreyectivas. Y esto es importante. Observemos el siguiente teorema.

Teorema 13.0

Para conjuntos finitos, son ciertas las siguientes afirmaciones:

0. $A \subseteq B \leftrightarrow$ existe una aplicación inyectiva $f : A \longrightarrow B \leftrightarrow \text{card}\, A \leq \text{card}\, B$;
1. $A \subset B \leftrightarrow$ existe una aplicación inyectiva y no sobreyectiva $f : A \longrightarrow B \leftrightarrow \text{card}\, A < \text{card}\, B$;
2. $A = B \leftrightarrow$ existe una aplicación biyectiva $f : A \longrightarrow B \leftrightarrow \text{card}\, A = \text{card}\, B$.

Ninguna de estas afirmaciones es cierta para conjuntos infinitos. En efecto:

0. g: $\mathbb{N} \longrightarrow \mathbb{N}_{\text{CUAD}}$, definida por $g(n) = n^2$ es inyectiva, pero, $\mathbb{N} \not\subseteq \mathbb{N}_{\text{CUAD}}$;
1. $f : H \longrightarrow H$, definida por $f(h_i) = h_{i+n}$, es inyectiva y no sobreyectiva, pero $H \not\subset H$;
2. g es biyectiva, pero $\mathbb{N} \neq \mathbb{N}_{CUAD}$.

Algo que caracteriza[1] a todo conjunto infinito es la existencia de una biyección entre él y algún subconjunto propio suyo[2]. Por ejemplo, $\mathbb{N}$ es infinito porque, en realidad, g es una biyección.[3]

[o] Pues, desplazando, para toda habitación n, a las personas que ocupan la habitación n a la habitación de número doble que la original; de este modo, quedan libres todas las habitaciones impares, que son infinitas, y se pueden alojar en ellas el número infinito de personas que quería hospedarse. La aplicación sería $g : H \longrightarrow H$, definida por $g(h_i) = h_{2i}$.

[1] *Cfr. infra* definición 13.7 (pág. 723 de esta edición).

[2] Si bien es la definición de conjunto infinito según DEDEKIND, desligada de ella aparece en textos referida como la *caracterización biyectiva propia*.

[3] En 1638, GALILEO refiere explícitamente esta correspondencia entre los números naturales y sus cuadrados. Aún más, parece que los estoicos —quizás CRISIPO de Solos (s. III, a. C.)— conjeturaban la existencia de tales correspondencias para cualquier conjunto infinito.

Observamos que el problema está en el «si», no en el «sólo si». Es por esto que se satisface lo que afirma el siguiente teorema.

Teorema 13.1

Para conjuntos infinitos, son ciertas las siguientes afirmaciones:

0. si $X \subseteq Y$, entonces existe una aplicación inyectiva $f : X \longrightarrow Y$;
1. si $X \subset Y$, entonces existe una aplicación inyectiva y no sobreyectiva, $f : X \longrightarrow Y$, y
2. si $X = Y$, entonces existe una aplicación biyectiva, $f : X \longrightarrow Y$.

§ 13.1 Cardinalidad

En este subcapítulo extendemos la noción de cardinal de un conjunto a conjuntos infinitos. El cardinal de un conjunto finito es su número de elementos. Pero, hablar de «número de elementos» entre conjuntos infinitos, puede crearnos cierta confusión: parece que tenemos claro que hay más elementos en el conjunto de los naturales, que en el de los naturales pares (incluso pudiésemos atrevernos a decir que el doble); sin embargo, como hemos visto en el ejemplo del hotel de HILBERT, debería haber el mismo número, pues todos los huéspedes del hotel (tantos como números naturales) han sido alojados en las habitaciones pares.

§ 13.1.0 Equipotencia

Definición 13.0 (Conjuntos equipotentes).— (BOLZANO, 1851; CANTOR, 1878). Decimos que dos conjuntos X e Y son *equipotentes* si, y sólo si, existe una aplicación biyectiva entre ellos. Pudiésemos utilizar la notación de aplicaciones[4], si bien simplificamos y, en adelante, $X \approx Y$ designa la equipotencia de X e Y.

Ejemplo 374

Demostremos que $\mathbb{Z}^+ \approx \mathbb{Z}^+ \setminus \{1\}$.

Resolución.— En efecto, $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+ \setminus \{1\}$, definida por $f(n) = n + 1$ es una biyección entre ellos (esto es lo que ocurre en el primer caso de la historia del hotel del infinito). ■

Ejemplo 375

Demostremos que $\mathbb{Z}^+ \approx \mathbb{Z}^+ \setminus \{1, \ldots, k\}$.

[4] Inyectiva: $\rightarrowtail$ o $\hookrightarrow$; sobreyectiva: $\twoheadrightarrow$; biyectiva: $\rightarrowtail\!\!\!\!\twoheadrightarrow$.

Resolución.— En efecto, en general, $\mathbb{Z}^+$ es equipotente a $\mathbb{Z}^+$ menos un número finito de elementos cualesquiera; no se pierde generalidad en suponer que este número finito está al principio, así $\mathbb{Z}^+ \approx \mathbb{Z}^+ \setminus \{1, \ldots, k\}$, debido a que $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+ \setminus \{1, \ldots, k\}$, definida por $f(n) = n + k$, es una biyección entre ellos. (esto es lo que ocurre en el segundo caso de la historia del hotel del infinito, con $k = 5$). ■

Ejemplo 376

Demostremos que $\mathbb{Z}^+ \approx \text{Pares}^+$.

Resolución.— En efecto, $f : \mathbb{Z}^+ \longrightarrow \text{Pares}^+$, definida por $f(n) = 2n$, es una biyección entre ellos (esto proporciona la solución para acomodar a los infinitos huéspedes). ■

De existir el conjunto de todos los conjuntos, la *equipotencia* (en palabras de CANTOR, y *equinumerosidad*, en palabras de FREGE) sería una relación de equivalencia en él, esto es, una relación de equivalencia en cualquier conjunto de conjuntos.

Teorema 13.2

Dados tres conjuntos X, Y y Z, se satisface:

0. $X \approx X$ (reflexiva);
1. si $X \approx Y$, entonces $Y \approx X$ (simétrica);
2. si $X \approx Y$ y $Y \approx Z$, entonces $X \approx Z$ (transitiva).

§ 13.1.1 Cardinal

Llamábamos *cardinal* (o, sinónimamente, *potencia*) de un conjunto finito al número de sus elementos. En el caso de conjuntos infinitos, nos limitaremos a decir que dos conjuntos tienen igual cardinal o potencia precisamente si son equipotentes, esto es, si, y sólo si, existe una aplicación biyectiva entre ellos. Representamos el cardinal de un conjunto X por $|X|$ (o, sinónimamente, $\text{card}(X)$, $\#X$, $\bar{X}$ o $\bar{\bar{X}}$ —esta última notación se debe a CANTOR—).

Como ya comentábamos, hablar de «número de elementos» entre conjuntos infinitos puede resultar paradójico. La solución no es difícil: *no hablaremos de «número de elementos» en el caso de conjuntos infinitos*.

§ 13.1.2 Ordenación de cardinales

Definición 13.1 (Relación de menor o igual potencia).— Dados dos conjuntos X e Y, decimos que el conjunto X está *dominado* por el conjunto Y (o, sinónimamente, que X es de *potencia menor o igual*

que Y o que Y es *al menos tan potente* como X), y notamos $X \precsim Y$, si, y sólo si, existe una aplicación inyectiva de X en Y.

Podremos definir, entonces, un orden parcial entre cardinales,

$$|X| \leq |Y|, \text{ si, y sólo si, } X \precsim Y,$$

esto es, si $\mathfrak{x}$ e $\mathfrak{y}$ son dos cardinales y X e Y, dos conjuntos, tales que $|X| = \mathfrak{x}$ e $|Y| = \mathfrak{y}$, entonces

$$\mathfrak{x} \leq \mathfrak{y}, \text{ si, y sólo si, } X \precsim Y.$$

Definición 13.2 (Relación de menor potencia).— Dados dos conjuntos X e Y, tales que $X \precsim Y$ y $X \not\approx Y$, decimos que X es de *menor cardinal*(idad) (o, sinónimamente, *menor potencia*) que Y. Esto equivale a que, existiendo aplicaciones inyectivas de X en Y, ninguna es biyectiva; lo notaremos por $X \prec Y$.

Así definimos un orden estricto entre cardinales,

$$|X| < |Y|, \text{ si, y sólo si, } X \prec Y,$$

es decir, si $\mathfrak{x}$ e $\mathfrak{y}$ son dos cardinales y X e Y, dos conjuntos, tales que $|X| = \mathfrak{x}$ e $|Y| = \mathfrak{y}$, entonces

$$\mathfrak{x} < \mathfrak{y}, \text{ si, y sólo si, } (\mathfrak{x} \leq \mathfrak{y}) \wedge (\mathfrak{x} \neq \mathfrak{y}).$$

De existir el conjunto de todos los cardinales, $\leq$ sería una relación de orden total en él; en cualquier caso, es una relación de orden total en cualquier conjunto de cardinales.

(Quizás esto se entienda mejor una vez estudiada la sucesión de infinitos[5]).

La demostración de la antisimétrica es todo un teorema en sí, llamado *teorema de* Cantor-Bernstein. (Nos puede servir de ejemplo para ver cómo se desarrolla la historia de la matemática. Este teorema fue demostrado por Cantor en 1897 —usando el axioma de elección[6]—, conjeturado por Schröder en 1896 y mal demostrado en 1898, demostración corregida por él, en 1911; demostrado sin axioma de elección por Bernstein, en 1898 (demostración publicada por Borel, en 1898).

[5] *Cfr. infra* § 13.11 (pág. 744 de esta edición).
[6] *Cfr. infra* § 14.3.0 (pág. 763 de esta edición).

§ 13.2 El conjunto $\mathbb{N}$ de los números naturales

Planteémonos, en este momento, una definición constructiva, no axiomática, de $\mathbb{N}$.

Zermelo (1908) propuso que cada número natural sea el conjunto unitario de único elemento el número natural anterior:

$$\begin{array}{ccccccc}
\emptyset & \{\emptyset\} & \{\{\emptyset\}\} & \{\{\{\emptyset\}\}\} & \{\{\{\{\emptyset\}\}\}\} & \{\{\{\{\{\emptyset\}\}\}\}\} & \dots \\
| & | & | & | & | & | & \\
0 & 1 & 2 & 3 & 4 & 5 & \dots \\
| & | & | & | & | & | & \\
0 & \{0\} & \{1\} & \{2\} & \{3\} & \{4\} & \dots
\end{array}$$

Centrémonos, sin embargo, en la propuesta de John von Neumann (1923), en la que cada número natural es el conjunto de todos los números naturales menores que él,

$$\begin{array}{cccccc}
\emptyset & \{\emptyset\} & \{\emptyset,\{\emptyset\}\} & \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\} & \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\},\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}\} & \dots \\
| & | & | & | & | & \\
0 & 1 & 2 & 3 & 4 & \dots \\
| & | & | & | & | & \\
0 & \{0\} & \{0,1\} & \{0,1,2\} & \{0,1,2,3\} & \dots
\end{array}$$

Observemos que con la propuesta de Neumann,

$$\begin{aligned}
0 &\leftrightharpoons \emptyset, \\
1 &\leftrightharpoons \{\emptyset\}, \\
2 &\leftrightharpoons \{\emptyset,\{\emptyset\}\}, \\
3 &\leftrightharpoons \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}, \\
&\vdots
\end{aligned}$$

esto es,

$$\begin{aligned}
&0, \\
1 &\leftrightharpoons \{0\}, \\
2 &\leftrightharpoons \{0,1\}, \\
3 &\leftrightharpoons \{0,1,2\}, \\
&\vdots \\
n &\leftrightharpoons \{0,1,2,\dots,n-1\}, \\
&\vdots
\end{aligned}$$

es decir, un número natural es el conjunto formado por todos los números naturales anteriores[7]. Para evitar confusiones, sobre todo a nivel técnico, hay quien nota a estos conjuntos $N_1 = \{0\}$, $N_2 = \{0, 1\}, \ldots, N_n = \{0, \ldots, n-1\}, \ldots$

En este momento, $\mathbb{N}$ quedaría definido por extensión como la reunión de 0, 1, 2, 3, y así sucesivamente. Pero, ¿cómo pudiésemos definir el conjunto de todos los números naturales si no quisiésemos emplear expresiones imprecisas del estilo de «y así sucesivamente»?

Definición 13.3 (Número natural).— Entendemos por *sucesor de un conjunto* a, y notamos a^+ ó $a+1$, el conjunto $a^+ = a \cup \{a\}$. Decimos que a es un *conjunto inductivo* precisamente si $\emptyset \in a$, y $\forall x \in a$, $x^+ \in a$. Por definición, un *número natural* es un conjunto que pertenece a todo conjunto inductivo.

Teorema 13.3 (Principio de Inducción para $\mathbb{N}$))

0. $\mathbb{N}$ es un conjunto inductivo, que es subconjunto de cualquier otro conjunto inductivo, esto es, $\mathbb{N}$ es el menor conjunto inductivo (en el sentido de la inclusión).
1. Cualquier subconjunto inductivo de $\mathbb{N}$, coincide con $\mathbb{N}$.

Demostración.— En efecto, por la definición anterior,

0. claramente, $\emptyset \in \mathbb{N}$, y si $x \in \mathbb{N}$, entonces, x pertenece a cualquier conjunto inductivo, por lo que x^+ también pertenece a cualquier conjunto inductivo, así que, $x^+ \in \mathbb{N}$;
1. demostrado, pues afirma lo mismo que el apartado anterior. ■

§ 13.3 Conjuntos finitos e infinitos

§ 13.3.0 La infinitud según Tarski, Cantor y Dedekind

Definición 13.4 (Conjuntos finitos e infinitos según Tarski).— Un conjunto es *finito* si, y sólo si, toda familia no vacía de subconjuntos suyos tiene un elemento minimal. Un conjunto *infinito* es un conjunto no finito.

Ejemplo 377

El conjunto $\mathbb{N}$, de los números naturales, es infinito.

Resolución.— Sea la familia no vacía de subconjuntos de $\mathbb{N}$ dada por $A_0 = \mathbb{N}$, $A_1 = \mathbb{N} \setminus \{0\}$, $A_2 = \mathbb{N} \setminus \{0, 1\}$, $A_3 = \mathbb{N} \setminus \{0, 1, 2\}, \ldots, A_n = \mathbb{N} \setminus \{0, 1, 2, \ldots, n-1\}$, $A_{n+1} = \mathbb{N} \setminus \{0, 1, 2, \ldots, n\}$,

[7] Claro que la construcción de Neumann genera algunos efectos laterales no deseados, aunque no son dañinos ni paradójicos, e incluso, a veces, son convenientes, en posteriores desarrollos formales. Por ejemplo, según ella, se tiene que $0 \in 1 \in 2 \in 3 \in \ldots$, y que $0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq \ldots$

..., esto es, definida por $A_{n+1} = A_n \setminus \{n\}$. Como $\forall n \in \mathbb{N}$ se satisface $A_{n+1} \subset A_n$, no hay elementos minimales en la familia $\{A_i : i \in \mathbb{N}\}$ ordenada por inclusión (su diagrama de Hasse es infinito). ■

Teorema 13.4

0. $\emptyset$ es finito.
1. Todo conjunto unitario es finito.
2. Todo subconjunto de un conjunto finito es finito.
3. La intersección de dos conjuntos finitos es un conjunto finito.
4. La diferencia de dos conjuntos finitos es un conjunto finito.
5. La unión de dos conjuntos finitos es un conjunto finito.
6. Si X es finito y f es una función tal que $\operatorname{dom} f = X$ y $\operatorname{ran} f = Y$, entonces Y es finito.
7. Si X es finito y $X \approx Y$, entonces Y es finito.
8. Un conjunto es finito si, y sólo si, su conjunto potencia es finito.

Por cierto, respecto de la complementariedad, la siguiente definición.

Definición 13.5 (Conjunto cofinito).— Decimos que un conjunto es cofinito precisamente si su complementario es finito.

Ejemplo 378

Demostremos el teorema 13.4.2 (pág. 723), esto es, que todo subconjunto de un conjunto finito es finito.

Resolución.— Sean X y Y conjuntos, X finito e $Y \subseteq X$. Precisamente por esto último, toda familia F no vacía de subconjuntos de Y lo es de X y como X es finito, F tiene un elemento minimal y, por tanto, Y es finito. ■

Definición 13.6 (Conjuntos finitos e infinitos según Cantor).— Un conjunto es *finito* si, y sólo si, es equipotente a algún número natural. Un conjunto *infinito* es un conjunto no finito.

Actividad 13.0

Demostremos, utilizando la definición de Cantor, que el conjunto $\mathbb{N}$, de los números naturales, es infinito.

Definición 13.7 (Conjuntos finitos e infinitos según Dedekind).— Un conjunto es *infinito* si, y sólo si, es equipotente a algún subconjunto propio suyo[8]. Un conjunto es *finito* precisamente si es un conjunto no infinito, esto es, si, y sólo si, no es equipotente a ningún subconjunto propio suyo.

Teorema 13.5
Un conjunto es finito en el sentido de Tarski si, y sólo si, es finito en el sentido de Dedekind.

Teorema 13.6
Si X e Y son conjuntos finitos, entonces $X \times Y$ es finito.

Teorema 13.7
Si X e Y son conjuntos finitos, entonces el conjunto de todas las aplicaciones de X en Y, $Y^X = \{f : X \longrightarrow Y, f \text{ aplicación}\} = \{f : f \text{ es una función} \wedge \operatorname{dom} f = X \wedge \operatorname{ran} f \subseteq Y\}$ es un conjunto finito.

Ambas definiciones, independientes, están interrelacionadas. Fijémonos en la definición de conjunto finito de Cantor; claramente, cualquier número natural la satisface. Para que esta definición sea correcta, deberíamos demostrar que cualquier conjunto finito es equipotente a un *único* número natural. Es posible demostrarlo con el *principio de los cajones de* Dirichlet[9], que establece que si hay que distribuir n objetos en un número menor que n de cajones, entonces, en algún cajón hay

[8] Aunque en nuestra exposición aparece como un teorema, así fue como definió Dedekind un conjunto infinito, definición que publicó en 1887, aunque la envió a Cantor, en 1882 y a Schwarz y Weber varios años antes. En vez de definir los conjuntos infinitos, Peirce se refiere a los conjuntos finitos como aquéllos para los que no existía esa biyección. Quizás pueda antojársenos trivial esta diferencia, pero la cuestión es profunda, ¿existe en la realidad algún conjunto infinito? (Nadie ha encontrado ningún ejemplo, que sepamos). Es más, el número total de átomos del universo, se estima en 10^{80}, un número infinitamente pequeño y totalmente despreciable, nada, absolutamente nada comparado con infinito, y si, como parece, los átomos no pueden dividirse infinitamente, entonces, si no existen los conjuntos infinitos (al menos en nuestra realidad), ¿para qué definirlos (en nuestra realidad)? Incluso la neurobiología parece venir en nuestra ayuda (o confundirnos aún más) al lanzar hipótesis sobre la discretización de nuestra percepción sensorial.

Aunque es una discusión, a veces casi olvidada, no está de más, recordar el infinito potencial y actual según Aristóteles.

¿No sería, quizás, mejor definir un conjunto finito, pero infinitamente extensible (*fiex*), esto es, un conjunto que fuese creciendo a medida que sea necesario? Esto es realmente lo que ocurre en el curso del tiempo, por ejemplo, el conjunto de todos los programas escritos en lenguaje C, en esta realidad, era vacío, mucho antes de especificarse tal lenguaje, en alguno de los mundos de esta realidad. No es un conjunto infinito, ni lo será nunca, aunque sí es un conjunto *fiex*.

Sin embargo, somos capaces de imaginar un conjunto infinito, y pudiésemos afirmar, por tanto, su existencia, aunque también somos capaces de imaginar lo absurdo, lo contradictorio, lo contrario a la naturaleza, y esto, estrictamente, no puede existir.

Además de la definición, Dedekind [180] (§66) aportaba la siguiente «demostración» de la existencia de conjuntos infinitos: «El universo de mis pensamientos, esto es, la totalidad S de las cosas que pueden ser objeto de mi pensamiento, es infinito. En efecto, sea s un elemento de S, entonces, el pensamiento s', correspondiente al enunciado “s puede ser objeto de mi pensamiento” es también un objeto de S. Y, si consideramos a s' como la imagen $\phi(s)$ del elemento s, esta representación ϕ, aplicada a S, tendría la propiedad de que $S' = \phi(S)$ sería un subconjunto estricto de S. Habría, en efecto, en S, un elemento —por ejemplo, mi propio yo— que sería distinto de cualquier pensamiento s', y que, por lo tanto, no estaría contenido en S'. Es claro que, si a y b fueran elementos distintos de S, también serían distintas sus imágenes mediante ϕ, a' y b'. Por consiguiente, ϕ establecería una correspondencia biunívoca entre S y S'. Y, según eso, el conjunto S sería infinito, como queríamos demostrar». Dedekind afirma que consideraciones similares se encuentran en el libro póstumo de Bolzano.

[9] *Cfr. infra* teorema 19.25 (pág. 1144 de esta edición).

que introducir más de un objeto. Este principio no es más que la definición de conjunto finito de DEDEKIND.

Teorema 13.8 (Principio de los cajones para $\mathbb{N}$)
Ningún número natural es equipotente a un subconjunto propio de sí mismo.

De hecho, ambas definiciones de conjunto infinito coinciden suponiendo el *axioma de elección*[10].[11] El siguiente lema nos ayuda a demostrarlo.

Lema 13.0.— Si X es un conjunto que incluye un subconjunto numerable $Y = \{y_0, y_1, y_2, \ldots\}$, entonces X es un conjunto infinito de DEDEKIND.

Demostración.— La correspondencia

$$\begin{aligned} f : X \setminus \{y_0\} &\longrightarrow X \\ x &\longmapsto f(x) = \begin{cases} x & \text{si} \quad x \in X \setminus Y \\ y_i & \text{si} \quad x = y_{i+1} \end{cases} \end{aligned}$$

es una aplicación biyectiva entre el subconjunto propio $X \setminus \{y_0\}$ de X y X, por lo que X es equipotente a un subconjunto propio suyo y por consiguiente, X es un conjunto infinito de DEDEKIND. ■

Teorema 13.9
Las definiciones de CANTOR y DEDEKIND de conjunto infinito dan lugar a los mismos conjuntos.

Demostración.— Demostremos que [→] si un conjunto es infinito de DEDEKIND, entonces lo es de CANTOR y [←] recíprocamente, si un conjunto es infinito de CANTOR, entonces lo es de DEDEKIND.

→: Sea X un conjunto infinito de DEDEKIND, esto es, un conjunto equipotente a un subconjunto propio suyo. Razonemos *por contraposición*. Si X no fuese infinito de CANTOR es que sería finito de CANTOR y esto significaría que sería equipotente a un número natural n. Entonces, cualquier subconjunto propio S de X también sería finito, ocurriendo además que $|S| < |X| = n$, por lo que $S \not\approx X$; esto es, X no sería equipotente a ningún subconjunto propio suyo, en otras palabras, X no sería un conjunto infinito de DEDEKIND.

←: Sea X un conjunto infinito de CANTOR. Vamos a construir un subconjunto Y propio y numerable de X, pues el lema 13.0 (pág. 725 de esta edición) asegura que en tal caso, X es un conjunto infinito de DEDEKIND. ■

[10] *Cfr. infra* § 14.3.0 (pág. 763 de esta edición).
[11] *Cfr. v. gr.* HUNTER [181] (pág. 59).

Teorema 13.10 (Corolarios)

0. Cualquier conjunto finito es equipotente a un único número natural.
1. Ningún conjunto finito es equipotente a un subconjunto propio de sí mismo.
2. Ningún conjunto infinito es subconjunto de un conjunto finito.
3. Ningún conjunto infinito puede obtenerse como la unión de dos conjuntos finitos.

§ 13.3.1 Infinitud de $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$

Ejemplo 379

El conjunto $\mathbb{N}$, de los números naturales, es infinito.

Resolución.— Un conjunto es infinito precisamente si existe una biyección entre él y un subconjunto propio suyo (según DEDEKIND). Sea, por ejemplo, la correspondencia $f : \mathbb{N} \longrightarrow \mathbb{N} \setminus \{0\}$, definida por $n \longmapsto f(n) = n + 1$. Veamos que es una aplicación biyectiva. En efecto:

- f es aplicación si, y sólo si, $(\forall x \in \mathbb{N})$ $(\exists y \in \mathbb{N} \setminus \{0\})$ $(f(x) = y)$ $\wedge$ $(\forall x, x' \in \mathbb{N})$ $(x = x' \to f(x) = f(x'))$, lo cual es trivial, ya que dado $x \in \mathbb{N}$, por definición de f, existe $y_x = x + 1 \in \mathbb{N} \setminus \{0\}$, siendo este y_x único para cada x, es decir, que si $x = x'$, por definición de f, $f(x) = x + 1 = y_x = y_{x'} = x' + 1 = f(x')$;
- f es inyectiva si, y sólo si, $(\forall x, x' \in \mathbb{N})$ $(f(x) = f(x') \to x = x')$, lo cual es trivial por definición de f, pues si $f(x) = f(x')$, es decir, si $x + 1 = x' + 1$, entonces, $x = x'$;
- f es sobreyectiva si, y sólo si, $(\forall y \in \mathbb{N} \setminus \{0\})$ $(\exists x \in \mathbb{N})$ $(f(x) = y)$, lo cual también es trivial por definición de f, ya que dado y, $x = y - 1$ es tal que $f(x) = f(y - 1) = (y - 1) + 1 = y$. ■

Observación 13.3.0.— En realidad hay infinitas demostraciones de que $\mathbb{N}$ es un conjunto infinito; mismamente, variando el subconjunto propio y la biyección. Por ejemplo, la correspondencia

$$\begin{aligned} f : \mathbb{N} &\longrightarrow 23\mathbb{N} \\ n &\longmapsto f(n) = 23n \end{aligned}$$

es una aplicación biyectiva de $\mathbb{N}$ en un subconjunto propio suyo, luego $\mathbb{N}$ es infinito (según DEDEKIND). Observemos que, en particular, aseguramos que

$$\mathbb{N} \approx \{0, 23, 46, 69, 92, 115, 138, 161, 184, 207, 230, \dots\}.$$

Ejemplo 380

El conjunto de los números enteros $\mathbb{Z}$ es infinito.

Resolución.— En efecto, pues, por ejemplo, la correspondencia

$$\begin{array}{rcl} f:\mathbb{Z} & \longrightarrow & \mathbb{N} \\ z & \longmapsto & f(z)=\begin{cases} 2z & \text{si} \quad z>0 \\ -2z+1 & \text{si} \quad z\leq 0 \end{cases} \end{array}$$

es una aplicación biyectiva de $\mathbb{Z}$ en un subconjunto propio suyo, luego $\mathbb{Z}$ es infinito (según DEDEKIND). ■

Ejemplo 381

El conjunto de los números racionales $\mathbb{Q}$ es infinito.

Resolución.— En efecto, pues, por ejemplo, la correspondencia

$$\begin{array}{rcl} f:\mathbb{Q} & \longrightarrow & \mathbb{Q}^+ \\ q & \longmapsto & f(q)=\begin{cases} q+1 & \text{si} \quad q\geq 0 \\ \dfrac{1}{1-q} & \text{si} \quad q<0 \end{cases} \end{array}$$

es una aplicación biyectiva de $\mathbb{Q}$ en un subconjunto propio suyo, luego $\mathbb{Q}$ es infinito (según DEDEKIND). ■

§ 13.3.2 Infinitud de $\mathbb{R}$

Ejemplo 382

El conjunto de los números reales $\mathbb{R}$ es infinito.

Resolución.— En efecto, la correspondencia

$$\begin{array}{rcl} f:\mathbb{R} & \longrightarrow & (-1,1) \\ r & \longmapsto & f(r)=\dfrac{r}{1-r^2} \end{array}$$

es una aplicación biyectiva de $\mathbb{R}$ en un subconjunto propio suyo, luego $\mathbb{R}$ es infinito (según DEDEKIND). Notemos que, en particular, aseguramos que $\mathbb{R}\approx(-1,1)$. ■

Ejemplo 383

Dos intervalos cualesquiera, abiertos y no vacíos, de números reales, (a, b) y (c, d), son equipotentes, esto es, $\forall a, b, c, d \in \mathbb{R}$, si $a < b$ y $c < d$, entonces $(a, b) \approx (c, d)$.

Resolución.— En efecto, la correspondencia

$$\begin{array}{rcl} f : (a, b) & \longrightarrow & (c, d) \\ x & \longmapsto & f(x) = \dfrac{(c-d)x + ad - bc}{a-b} \end{array}$$

es una aplicación biyectiva. De aquí deducimos que también un intervalo real es un conjunto infinito, pues basta particularizar, por ejemplo, para $(a, b) \subset (c, d)$. ■

Ejemplo 384

El conjunto de números reales $\mathbb{R}$ es equipotente a cualquier intervalo de números reales abierto y no vacío, esto es, $\forall a, b \in \mathbb{R}$, si $a < b$, entonces $\mathbb{R} \approx (a, b)$.

Resolución.— En efecto, por el ejemplo 382 (pág. 727 de esta edición) y el ejemplo 383 (pág. 728 de esta edición), es posible razonar, como mínimo, de un par de formas:

0. utilizando la propiedad transitiva de la relación $\approx$;

1. sabemos, en particular, que las correspondencias dadas en el ejemplo 382 (pág. 727 de esta edición) y en el ejemplo 383 (pág. 728 de esta edición) son aplicaciones inyectivas, por lo que $\mathbb{R} \precsim (-1, 1) \precsim (a, b)$, y $(a, b) \precsim (-1, 1) \precsim \mathbb{R}$, de donde, por la transitividad de $\precsim$, $\mathbb{R} \precsim (a, b)$ y $(a, b) \precsim \mathbb{R}$, por lo que por el teorema de CANTOR-Bernstein, $\mathbb{R} \approx (a, b)$. ■

Ejemplo 385

El conjunto de números reales $\mathbb{R}$ es equipotente a cualquier intervalo de números reales cerrado y no vacío, esto es, $\forall a, b \in \mathbb{R}$, si $a < b$, entonces $\mathbb{R} \approx [a, b]$.

Resolución.— En efecto, como $[a, b] \subseteq \mathbb{R}$, se tiene que $[a, b] \precsim \mathbb{R}$, y como $\mathbb{R} \approx (a, b) \subseteq [a, b]$, también, $\mathbb{R} \precsim [a, b]$, así que, por el teorema de CANTOR-Bernstein, $\mathbb{R} \approx [a, b]$. ■

Ejemplo 386

El conjunto de números reales $\mathbb{R}$ es equipotente a $(0, 1)$, esto es, $\mathbb{R} \approx (0, 1)$.

Resolución.— Cierto es que en las observaciones precedentes no hemos explicitado la biyección, aunque en algunos casos hubiera bastado componer las biyecciones existentes. En el caso que nos ocupa, la aplicación biyectiva

$$\begin{aligned} f : (0,1) &\longrightarrow \mathbb{R} \\ x &\longmapsto f(x) = \frac{x-\frac{1}{2}}{x(x-1)} \end{aligned}$$

demuestra la equipotencia de $\mathbb{R}$ con $(0,1)$. ■

§ 13.4 Conjunto (infinito) numerable

En este subcapítulo estudiamos varias propiedades de los conjuntos equipotentes a $\mathbb{N}$, conjuntos que llamamos numerables.

Visto lo anterior, definir cardinal de un conjunto finito A, como el único número natural n tal que $A \approx n$, es equivalente a definirlo como el número de elementos de A. La definición de cardinal de un conjunto arbitrario —finito o no—, debe particularizarse en la anterior, cuando el conjunto sea finito, y además, debe verificar lo postulado por la relación de equipotencia, a saber, $|A| = |B| \leftrightarrow A \approx B$.

Por número cardinal entendemos cualquier número que sea el cardinal de algún conjunto. Parece claro que cualquier número natural es un número cardinal. Pero, por ser $\mathbb{N}$ un conjunto infinito[12], $|\mathbb{N}|$ no es un número natural[13] ya que no existe un número natural infinito.

Definición 13.8 (Cardinal del conjunto de números naturales).— Cantor eligió $\aleph_0$ para designar el cardinal de $\mathbb{N}$ —el signo $\aleph$ es «alef», la primera letra del alfabeto hebreo—.

Definición 13.9 (Conjunto numerable).— Decimos que un conjunto X es infinito numerable o, simplemente, numerable o que su potencia es numerable, si es equipotente a $\mathbb{N}$, es decir, si $|X| = \aleph_0$.

Definición 13.10 (Conjunto conumerable).— Decimos que un conjunto es conumerable precisamente si su complementario es numerable.

Observación 13.4.0.— En algunos textos se denomina *conjunto contable* a aquél cuyo cardinal es menor o igual que $\aleph_0$, o sea, al que es finito o numerable. En ellos, un conjunto conumerable se denomina *conjunto co-contable*.

[12] *Cfr. supra* ejemplo 379 (pág. 726 de esta edición).
[13] *Cfr. supra* teorema 13.6 (pág. 723 de esta edición).

§ 13.4.0 Numerabilidad de $\mathbb{Z}$

Numerabilidad de $\mathbb{Z}$ por definición de numerabilidad

Ejemplo 387

El conjunto de los enteros negativos $\mathbb{Z}^-$ es numerable.

Resolución.— En efecto, ya que, por ejemplo, la correspondencia

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{Z}^- \\ n &\longmapsto f(n) = -n \end{aligned}$$

es una aplicación biyectiva. ■

Ejemplo 388

El conjunto de los números enteros $\mathbb{Z}$ es numerable.

Resolución.— En efecto, pues, por ejemplo, la correspondencia

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{Z} \\ n &\longmapsto f(n) = \begin{cases} 0 & \text{si} \quad n = 0 \\ (-1)^n \lfloor \frac{n+1}{2} \rfloor & \text{si} \quad n > 0 \end{cases} = \begin{cases} \frac{n}{2} & \text{si} \quad n \text{ es par} \\ \frac{-(n+1)}{2} & \text{si} \quad n \text{ es impar} \end{cases} \end{aligned}$$

es una aplicación biyectiva. ■

Observación 13.4.1.— Establecer una biyección entre los conjuntos $\mathbb{N}$ y A corresponde a encontrar un procedimiento efectivo de numeración de los elementos del conjunto A, esto es, a que los elementos de A puedan disponerse como una sucesión $\langle a_0, a_1, a_2, \ldots \rangle$. Por ejemplo, la aplicación biyectiva dada en el ejemplo 388 (pág. 730 de esta edición), corresponde al procedimiento de enumeración que ordena $\mathbb{Z}$ así

$$\begin{aligned} \mathbb{Z} &= \{f(0), f(1), f(2), f(3), f(4), \ldots\} \\ &= \{0, -1, 1, -2, 2, -3, 3, -4, 4, \ldots\}. \end{aligned}$$

Notemos, pues, que hemos definido un nuevo orden en $\mathbb{Z}$, un orden con el que existe un primer elemento en $\mathbb{Z}$, a saber, 0, un segundo, -1, un tercero, 1, un cuarto, -2, etc. —observemos que según este nuevo orden, 1 precede a -2 (es menor que -2, pudiésemos decir), así notando este nuevo orden por $<_f$, tenemos que

$$0 <_f -1 <_f 1 <_f -2 <_f 2 <_f -3 <_f 3 <_f -4 <_f 4 <_f \ldots$$

Observación 13.4.2.— La definición de numerabilidad es independiente de que se considere o no 0 como número natural, ya que $\mathbb{N} \approx \mathbb{Z}^+$, pues $f(n) = n + 1$ es biyección entre ellos. En realidad, podría formularse para cualquier subconjunto infinito de $\mathbb{N}$ —debido a la equipotencia entre ellos[14].

Teorema 13.11
Todo subconjunto infinito B de un conjunto numerable A es numerable.

Demostración.— Como A es numerable, sus elementos pueden disponerse como una sucesión $A = \{a_0, a_1, a_2, \ldots\}$. Procedemos a construir inductivamente B: sea n_0 el menor natural tal que $a_{n_0} \in B$, y sea n_k el menor natural, mayor que n_{k-1}, tal que $a_{n_k} \in B$. De este modo, $B = \{a_{n_0}, a_{n_1}, \ldots, a_{n_k}, \ldots\}$. ■

Numerabilidad de $\mathbb{Z}$ como unión finita de numerables

Teorema 13.12
La unión de un conjunto finito y un conjunto numerable es numerable.

Demostración.— En efecto, sean $A = \{a_0, a_1, a_2, \ldots\}$, numerable y $B = \{b_0, b_1, \ldots, b_{n-1}\}$, entonces la correspondencia $f : A \cup B \longrightarrow \mathbb{N}$, definida por $f(b_i) = i$ y $f(a_i) = n+i$, es una aplicación biyectiva. ■

Teorema 13.13
La intersección de un conjunto finito y un conjunto numerable es finita.

Actividad 13.1

Demostremos el teorema 13.13 (pág. 731 de esta edición), esto es, que la intersección de un conjunto finito y un conjunto numerable es finita.

Teorema 13.14 (Numerabilidad de la unión finita)
La unión finita de conjuntos numerables es numerable.

Demostración.— En efecto, sean $A = \{a_0, a_1, a_2, \ldots\}$ y $B = \{b_0, b_1, b_2, \ldots\}$ numerables, entonces, $A \cup B = \{a_0, b_0, a_1, b_1, a_2, b_2, \ldots\}$ y la aplicación $f : A \cup B \longrightarrow \mathbb{N}$, definida por $f(a_i) = 2i$, $f(b_i) = 2i + 1$, es biyectiva. ■

Ejemplo 389

El conjunto $\mathbb{Z}$ de los números enteros es numerable.

[14] *Cfr. infra* teorema 13.11 (pág. 731 de esta edición).

Resolución.— Así es, pues, por ejemplo, $\mathbb{Z} = \mathbb{Z}^- \cup \mathbb{N}$, esto es, $\mathbb{Z}$ es unión finita de dos conjuntos numerables y por el teorema 13.14 (pág. 731 de esta edición) es numerable. ■

Numerabilidad de $\mathbb{Z}$ como unión numerable de conjuntos finitos

Teorema 13.15
La unión numerable de conjuntos finitos es numerable.

Demostración.— En efecto, sean $A_i = \{a_{i0}, a_{i1}, a_{i2}, \ldots, a_{in_i}\}$ ($i \in \mathbb{N}$), entonces la correspondencia $f : \bigcup_{i\in\mathbb{N}} A_i \longrightarrow \mathbb{N}$, definida por $f(a_{0j}) = j$ y $f(a_{ij}) = \sum_{k=0}^{i-1} n_k + k + j$ (esto es, $f(a_{1j}) = n_0 + 1 + j$, $f(a_{2j}) = n_0 + 1 + n_1 + 1 + j$, $f(a_{3j}) = n_0 + 1 + n_1 + 1 + n_2 + 1 + j, \ldots$), es una aplicación biyectiva. ■

Ejemplo 390

El conjunto $\mathbb{Z}$ de los números enteros es numerable.

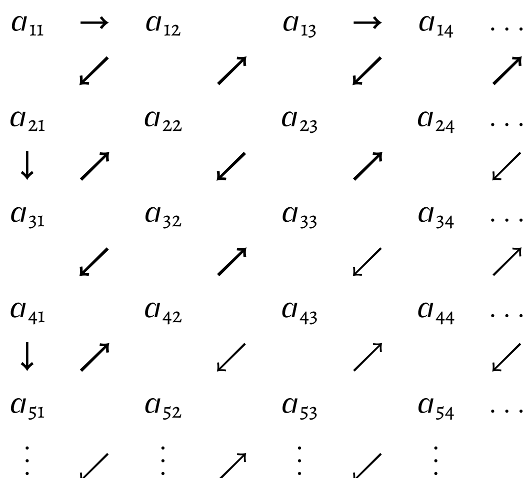
Resolución.— Así es, pues, por ejemplo, $\mathbb{Z} = \{0\} \cup \{-1\} \cup \{1\} \cup \{-2\} \cup \{2\} \cup \{-3\} \cup \ldots$, esto es, $\mathbb{Z}$ es unión numerable de conjuntos finitos y por el teorema 13.15 (pág. 732 de esta edición) es numerable. ■

§ 13.4.1 Numerabilidad de $\mathbb{Q}$

Numerabilidad de $\mathbb{Q}$ como unión numerable de numerables

Teorema 13.16 (Numerabilidad de la unión numerable)
La unión numerable de conjuntos numerables es numerable.

Demostración.— En efecto, sean $A_1 = \{a_{11}, a_{12}, a_{13}, \ldots\}$, $A_2 = \{a_{21}, a_{22}, a_{23}, \ldots\}$, $A_3 = \{a_{31}, a_{32}, a_{33}, \ldots\}$, etc. Ordenemos el conjunto unión según las flechas



esto es,

$$\bigcup_{n\in\mathbb{N}} A_n = \{a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, a_{14}, a_{23}, a_{32}, a_{41}, \ldots\}$$

es decir, primero, a_{11}, cuyos subíndices suman dos, después, a_{12}, a_{21}, cuyos subíndices suman 3, comenzando por el que tiene menor el primer subíndice, a continuación, a_{13}, a_{22}, a_{31}, esto es, aquéllos cuyos subíndices suman 4, comenzando por el que tiene menor el primer subíndice, etc. Pues bien, la correspondencia

$$\begin{array}{rcl} f : \bigcup_{n\in\mathbb{Z}^+} A_n & \longrightarrow & \mathbb{N} \\ a_{ij} & \longmapsto & f(a_{ij}) = i + \dfrac{(i+j-1)(i+j-2)}{2} \end{array}$$

es una aplicación biyectiva. ■

Ejemplo 391

El conjunto $\mathbb{Q}$ de los números racionales es numerable.

[AIC 7.7.2017:2].

Resolución.— En efecto, pues, por ejemplo, es posible expresar $\mathbb{Q}$ como la unión numerable

$$\mathbb{Q} = A_1 \cup A_2 \cup \ldots \cup A_n \cup \ldots,$$

donde cada

$$A_i = \left\{0, \frac{-1}{i}, \frac{1}{i}, \ldots, \frac{-k}{i}, \frac{k}{i}, \ldots\right\}$$

es numerable, ya que, por ejemplo, la correspondencia

$$\begin{array}{rcl} f : \mathbb{Z} & \longrightarrow & A_i \\ n & \longmapsto & f(n) = \dfrac{n}{i} \end{array}$$

es una aplicación biyectiva. Observemos que A_i es el conjunto de todos los números racionales que tienen el mismo denominador i. ■

Ejemplo 392

¿Alguna biyección explícita de $\mathbb{Z}^+$ en $\mathbb{Q}^+$?

Resolución.— Veamos un ejemplo de una tal biyección explícita. Para $n \in \mathbb{Z}^+$, por el teorema fundamental de la aritmética —*vid. infra* teorema 18.17 (pág. 959 de esta edición)—, $n = \prod_{i=1}^{\infty} p_i^{a_i}$, donde

p_i son los números primos en orden —$p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. La correspondencia

$$\begin{array}{rcl} q_+ : \mathbb{Z}^+ & \longrightarrow & \mathbb{Q}^+ \\ n & \longmapsto & q_+(n) = \prod_{i=1}^{\infty} p_i^{z(a_i)} \end{array}$$

donde $z : \mathbb{N} \longrightarrow \mathbb{Z}$, es la f definida en el ejemplo 388 (pág. 730 de esta edición) —esto es, $z(0) = 0$, $z(1) = -1$, $z(2) = 1$, $z(3) = -2$, $z(4) = 2$, $z(5) = -3$, $z(6) = 3, \ldots$—, es una aplicación biyectiva. Así, por ejemplo, $q_+^{-1}(1/4) = q_+^{-1}(2^{-2}) = q_+^{-1}(2^{z(3)}) = 2^3 = 8$. ■

Numerabilidad de $\mathbb{Q}$ como subconjunto infinito de un producto cartesiano finito de numerables

Teorema 13.17 (Numerabilidad del producto cartesiano)
El producto cartesiano finito de conjuntos numerables es numerable.

Demostración.— Pudiésemos hacer esta demostración como actividad práctica (✍), pues su elaboración es muy parecida a la anterior; sean $A = \{a_0, a_1, a_2, \ldots\}$ y $B = \{b_0, b_1, b_2, \ldots\}$, numerables, escribimos $A \times B$ siguiendo las diagonales, como en la demostración del teorema 13.16 (pág. 732 de esta edición),

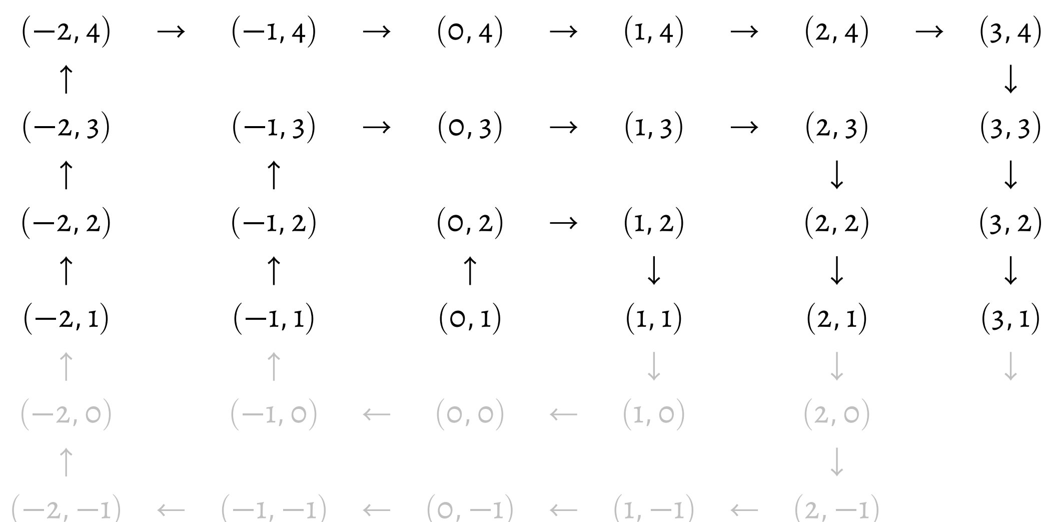
$$\begin{array}{ccccccccc}
(a_0, b_0) & \rightarrow & (a_0, b_1) & & (a_0, b_2) & \rightarrow & (a_0, b_3) & & \ldots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
(a_1, b_0) & & (a_1, b_1) & & (a_1, b_2) & & (a_1, b_3) & & \ldots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
(a_2, b_0) & & (a_2, b_1) & & (a_2, b_2) & & (a_2, b_3) & & \ldots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & \\
(a_3, b_0) & & (a_3, b_1) & & (a_3, b_2) & & (a_3, b_3) & & \ldots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & \\
(a_4, b_0) & & (a_4, b_1) & & (a_4, b_2) & & (a_4, b_3) & & \ldots \\
\vdots & \swarrow & \vdots & \nearrow & \vdots & \swarrow & \vdots & &
\end{array}$$

esto es, $A \times B = \{(a_0, b_0), (a_0, b_1), (a_1, b_0), (a_0, b_2), (a_1, b_1), (a_2, b_0), (a_0, b_3), \ldots\}$. ■

Ejemplo 393

$\mathbb{Q}$ es numerable.

Resolución.— Esto es así, pues, por ejemplo, pudiésemos expresar $\mathbb{Q}$ como un subconjunto infinito de $\mathbb{Z} \times \mathbb{Z}^+ = \{\langle p, q \rangle : p \in \mathbb{Z} \wedge q \in \mathbb{Z}^+\}$ que por el teorema 13.17 (pág. 734 de esta edición) es numerable —por lo que $\mathbb{Q}$ es numerable por ser un subconjunto infinito de un conjunto numerable —*cfr. supra* teorema 13.11 (pág. 731 de esta edición)—. Observemos que es posible recorrer en «casi-espiral» el semiplano entero $\mathbb{Z} \times \mathbb{Z}^+$,



como vemos, comenzando por $(0, 1)$ y siguiendo por $(0, 2)$, $(1, 2)$, $(1, 1)$, $(-1, 1)$, $(-1, 2)$, $(-1, 3)$, $(0, 3)$, $(1, 3)$, $(2, 3)$, ... ■

Sobre la numerabilidad del producto cartesiano aún queda algo por decir.

Teorema 13.18
El producto cartesiano numerable de conjuntos numerables es no numerable.

§ 13.4.2 Numerabilidad y buen orden

Teorema 13.19
Todo conjunto numerable está bien ordenado, esto es, en todo conjunto numerable puede definirse una relación de buen orden.

§ 13.5 Infinitud de $\mathbb{R}$: la potencia del continuo

CANTOR designa por $\mathfrak{c}$ la *potencia del continuo*, esto es, el cardinal del conjunto $\mathbb{R}$, del que ya demostramos su infinitud[15]. En este subcapítulo proporcionamos la demostración de CANTOR de que $\aleph_0 < \mathfrak{c}$.

A partir de una relación diádica R en $\mathbb{N}$, y un número $m \in \mathbb{N}$, definimos la relación monádica

$$R_m(n) \leftrightarrow R(n, m).$$

[15] *Cfr. supra* ejemplo 382 (pág. 727 de esta edición).

Teorema 13.20 (Lema diagonal de CANTOR)
Sea P una relación diádica y sea Q la relación monádica definida por $(\forall n \in \mathbb{N})(Q(n) \leftrightarrow \neg P(n,n))$, entonces $\forall n \in \mathbb{N}$, $P_n \neq Q$.

Demostración.— Por reducción al absurdo. En efecto, si existiese algún $n \in \mathbb{N}$ tal que $P_n = Q$, entonces, como por un lado, $P(n,n) \leftrightarrow P_n(n)$ y, por otro, $Q(n) \leftrightarrow \neg P(n,n)$, al ser igual P_n y Q se llegaría a la fórmula insatisfactible $P(n,n) \wedge \neg P(n,n)$; por tanto, por reducción al absurdo, $\forall n \in \mathbb{N}$, $P_n \neq Q$. ■

La relación monádica Q se conoce como *relación antidiagonal* respecto de la relación diádica P y al conjunto $\{n : Q(n)\}$, como *conjunto antidiagonal*.

Teorema 13.21 (Lo numerable está estrictamente dominado por lo continuo)
$\aleph_0 < \mathfrak{c}$.

Demostración.— Este es un ejemplo de demostración constructiva —*cfr. infra* § 7.6 (pág. 469 de esta edición)—.

Sabemos —*cfr. supra* § 13.3.2 (pág. 728 de esta edición) y precedentes— que $\mathbb{R} \approx (0,1)$; bastará, pues, razonar para este intervalo. Imaginemos que tenemos enumerados todos los números reales del intervalo $(0,1)$ y consideremos sus representaciones decimales; es posible definir un número real distinto de todos los de tal enumeración, simplemente, haciendo que el dígito n del nuevo número sea distinto del dígito n del número real que está en la posición n de la enumeración. Para ello usaremos el lema diagonal de CANTOR —*cfr. supra* § 13.20 (pág. 736 de esta edición)—. Concretamos, supongamos que existe una enumeración de los números reales, $r_0, r_1, r_2, r_3, \ldots$ de $(0,1)$,

$$\begin{aligned} r_0 &= 0, a_{00}a_{01}a_{02}a_{03}\ldots \\ r_1 &= 0, a_{10}a_{11}a_{12}a_{13}\ldots \\ r_2 &= 0, a_{20}a_{21}a_{22}a_{23}\ldots \\ r_3 &= 0, a_{30}a_{31}a_{32}a_{33}\ldots \\ &\vdots \end{aligned}$$

y pensemos en un número real r cuya representación decimal satisfaga que su primer dígito decimal sea distinto del primer dígito decimal a_{00} de r_0, que su segundo dígito decimal sea distinto del segundo dígito decimal a_{11} de r_1, que su tercer dígito decimal sea distinto del tercer dígito decimal a_{22} de r_2, etc. Esto hará que r sea distinto de r_0 en su primer dígito decimal, distinto de r_1 en su segundo dígito decimal, distinto de r_2 en su tercer dígito decimal, etc.

$$\begin{array}{cccccccc} r = & \overline{\underline{0,}} & \overline{\underline{\neq a_{00}}} & \overline{\underline{\neq a_{11}}} & \overline{\underline{\neq a_{22}}} & \overline{\underline{\neq a_{33}}} & \ldots \\ & & \Downarrow^{16} & \Downarrow^{16} & \Downarrow^{16} & \Downarrow^{16} & \\ & & r \neq r_0 & r \neq r_1 & r \neq r_2 & r \neq r_3 & \ldots \end{array}$$

Por ejemplo, sea el número real $r = 0, a_0a_1a_2\ldots$, donde $a_i = a_{ii} + 1$ si $a_{ii} < 9$ y $a_i = a_{ii} - 1$ si $a_{ii} = 9$. Se tiene entonces lo dicho, esto es, para todo $n \in \mathbb{N}$, r es distinto de r_n en el dígito que ocupa la posición n. ■

[EFO 1.6.2017:2].

§ 13.6 Producto cartesiano de conjuntos equipotentes a $\mathbb{R}$

«Lo veo, pero no lo creo», escribió CANTOR a DEDEKIND el 29 de junio de 1877, tras descubrir que el *cuadrado unitario* $[0,1] \times [0,1]$ es equipotente al *segmento unitario* $[0,1]$.

Teorema 13.22
$[0,1] \approx [0,1]^2$.

Demostración.— Demostremos que $[0,1] \approx [0,1] \times [0,1]$ por *doble dominancia*.

$\precsim$: La correspondencia

$$\begin{array}{rcl} f : [0,1] & \longrightarrow & [0,1] \times [0,1] \\ r = 0, a_0a_1\ldots a_{2n}a_{2n+1}\ldots & \longmapsto & f(r) = \langle 0, a_0a_2\ldots a_{2n}\ldots, \ 0, a_1a_3\ldots a_{2n+1}\ldots \rangle \end{array}$$

es una aplicación inyectiva.

$\succsim$: La correspondencia

$$\begin{array}{rcl} g : [0,1] \times [0,1] & \longrightarrow & [0,1] \\ \langle r, s\rangle = \langle 0, r_0r_1\ldots r_n\ldots, \ 0, s_0s_1\ldots s_n\ldots\rangle & \longmapsto & g(\langle r, s\rangle) = 0, r_0s_0r_1s_1\ldots r_ns_n\ldots \end{array}$$

es una aplicación inyectiva.

Como $[0,1] \precsim [0,1] \times [0,1]$ y $[0,1] \times [0,1] \precsim [0,1]$, entonces de la antisimétrica de $\precsim$ —teorema de CANTOR— que $[0,1] \approx [0,1] \times [0,1]$. ■

Abreviemos, como es habitual, el producto cartesiano con notación de potencia, por ejemplo, $[0,1] \times [0,1] \times \overset{n}{\ldots} \times [0,1]$ por $[0,1]^n$.

Teorema 13.23
$\forall n \in \mathbb{Z}^+, [0,1] \approx [0,1]^n$.

---

[16] Para poder afirmar que dos números reales son distintos si, y sólo si, difieren en una cifra decimal, debemos quedarnos con una de las dos expresiones distintas $0, d_0d_1\ldots d_k999\ldots$ y $0, d_0d_1\ldots d_{k+1}000\ldots$ del mismo número real (por ejemplo, $0,0123456999\ldots = 0,0123457000\ldots$); decidimos quedarnos con la primera, esto es, con que no existen los números de la forma $0, d_0d_1\ldots d_{k+1}000\ldots$

Demostración.— La demostración del teorema 13.22 (pág. 737 de esta edición) se extiende de manera natural para el caso del cubo unitario, $[0,1] \approx [0,1]^3$ y del hipercubo unitario, $[0,1] \approx [0,1]^n$. ■

Observación 13.6.0.— $\mathbb{R} \approx [0,1] \approx [0,1]^n \approx \mathbb{R}^n$.

§ 13.7 Cardinalidad de la potencia de un conjunto

Por ahora, sabemos que los conjuntos $\mathbb{N}$, $\mathbb{Z}$ y $\mathbb{Q}$ tienen la misma potencia, la numerable, $\aleph_0$. Se puede demostrar que sus conjuntos potencia, $2^{\mathbb{N}}$, $2^{\mathbb{Z}}$ y $2^{\mathbb{Q}}$, respectivamente, tienen la misma potencia, la del continuo, $\mathfrak{c}$. El siguiente teorema demuestra el caso particular de $2^{\mathbb{N}}$.

Teorema 13.24
$2^{\aleph_0} = \mathfrak{c}$,
esto es, $2^{\mathbb{N}} \approx \mathbb{R}$, o sea, que $|2^{\mathbb{N}}| = 2^{|\mathbb{N}|}$.

Demostración.— Ofrecemos dos, alternativas.

Vía 0.

Sabemos —*cfr. supra* ejemplo 385 (pág. 728 de esta edición)— que $[0,1] \approx \mathbb{R}$, por lo que basta demostrar que $[0,1] \approx 2^{\mathbb{N}}$. Hagámoslo construyendo una aplicación biyectiva entre ambos. Consideremos los números reales de $[0,1]$ representados en el sistema binario exigiendo que la sucesión de bits no termine en una sucesión infinita de unos, para que así la representación sea única. La correspondencia

$$\begin{array}{rcl} f : [0,1] & \longrightarrow & 2^{\mathbb{N}} \\ r = 0, d_0 d_1 d_2 \ldots & \longmapsto & f(r) = \{n \in \mathbb{N} : d_n = 1\} \end{array}$$

es una aplicación biyectiva. De paso, su inversa es

$$\begin{array}{rcl} f^{-1} : 2^{\mathbb{N}} & \longrightarrow & [0,1] \\ S & \longmapsto & f^{-1}(S) = 0, d_0 d_1 d_2 \ldots \end{array}$$

siendo $\forall i \in \mathbb{N}$, $d_i = 1_S(i)$, donde 1_S es la función característica de S —*cfr. supra* ejemplo 12.7 (pág. 698 de esta edición)—.

Vía 1.

Demostremos que $2^{\mathbb{N}} \approx \mathbb{R}$ por *doble dominancia*.

$\precsim$: La correspondencia

$$\begin{array}{rcl} f : 2^{\mathbb{N}} & \longrightarrow & \mathbb{R} \\ S = \{n_0, n_1, n_2, \ldots\} & \longmapsto & f(S) = 0, d_0 d_1 d_2 \ldots \end{array}$$

siendo, $\forall i \in \mathbb{N}$, $d_i = 1$ si $i \in S$ y $d_i = 9$ si $i \notin S$, es una aplicación inyectiva.

$\gtrsim$: La correspondencia

$$\begin{array}{rcl} g : \mathbb{R} & \longrightarrow & 2^{\mathbb{N}} \\ r = n, d_0 d_1 d_2 \ldots & \longmapsto & g(r) = \{n, nd_0, nd_0 d_1, nd_0 d_1 d_2, \ldots\} \end{array}$$

es una aplicación inyectiva. ■

En realidad, este resultado se verifica para cualquier conjunto.

Teorema 13.25 (Cardinal del conjunto potencia)
El cardinal del conjunto potencia de un conjunto es $|2^A| = 2^{|A|}$.

Demostración.— El número de aplicaciones que pueden definirse entre dos conjuntos, $f : A \longrightarrow B$, se calcula como las variaciones con repetición, $VR(|B|, |A|)$, esto es, $|B|^{|A|}$. Sean $\mathbb{Z}_2^A$ (el conjunto de todas las aplicaciones $f : A \longrightarrow \mathbb{Z}_2$) y $g : 2^A \longrightarrow \mathbb{Z}_2^A$, definida por $g(B) = 1_B$, donde 1_B es la función característica de B, esto es, $1_B(x) = 1$ si $x \in B$ y $1_B(x) = 0$ si $x \notin B$. No es difícil demostrar que g es biyectiva. Por tanto, $|2^A|$ es $|\mathbb{Z}_2|^{|A|}$, esto es, $|2^A| = 2^{|A|}$. ■

Observación 13.7.0.— Algo que hemos admitido, sin más, para conjuntos finitos, es la existencia del conjunto potencia. Es admisible razonar que existe, proporcionando un método efectivo de construcción del mismo, que además termina en tiempo finito. Sin embargo, para conjuntos infinitos, formalmente, la situación no es obvia. De hecho, cualquier axiomática conjuntista contienen algún axioma que implique tal existencia. En el caso de la axiomática de Zermelo-Fraenkel[17], se concreta en el axioma del conjunto potencia[18]: «Para todo conjunto existe su conjunto potencia», formalmente, $\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x)$.

§ 13.8 Teorema de Cantor

Pudiésemos pensar que los únicos cardinales son $\aleph_0$ y $\mathfrak{c}$. Por el siguiente teorema, Cantor demuestra que hay infinitos cardinales mayores que el del continuo, proporcionando, además, una ley de formación de los mismos.

Teorema 13.26 (Cantor, 1891)
Para todo conjunto A, $|A| < 2^{|A|}$.

Demostración.— Para conjuntos finitos, es fácil demostrar, por ejemplo, por inducción, que $\forall n \in \mathbb{N}$, $|A| = n < 2^n = |2^A|$ (*cfr. infra* ejemplo 410 [pág. 805 de esta edición]). Para conjuntos infinitos, razonamos en dos fases: primero, demostramos que existe una inyección desde A a un

[17] *Cfr. infra* § 14.4 (pág. 765 de esta edición).
[18] *Cfr. infra* § 14.2.4 (pág. 760 de esta edición).

subconjunto propio de 2^A, por lo que $|A| \leq |2^A|$; a continuación, demostramos que no existe ninguna biyección entre A y 2^A, por lo que, $|A| \neq |2^A|$. Lo primero es trivial, basta tomar como subconjunto propio el conjunto de todos los subconjuntos, que tienen como único elemento, un elemento de A. Para demostrar lo segundo, razonamos por reducción al absurdo; suponemos que existe una biyección entre A y 2^A. Sea B el conjunto de todos los elementos de A, que no son elementos del subconjunto asignado a ellos por la biyección, o sea, $B = \{a \in A : a \notin f(a)\}$ y sea $b = f^{-1}(B)$. El elemento b debe estar o no estar en B; si $b \in B$, entonces, por definición de B, $b \notin f(B)$, esto es, $b \notin B$; por otro lado, si $b \notin B$, entonces, por definición de B, $b \in f(B)$, o sea, $b \in B$. Concluimos que no puede existir una biyección entre A y 2^A, y por tanto, $|A| \neq |2^A|$. ■

De este teorema deducimos, por ejemplo, la *regla de cálculo* $\mathfrak{c} < 2^{\mathfrak{c}}$.[19]

Ejemplo 394

Utilizando el teorema de CANTOR, demostremos por reducción al absurdo que no existe el conjunto de todos los conjuntos.

[Cubit 85].

Resolución.— Sea V el conjunto de todos los conjuntos, entonces, $|V| < |2^V|$, pero 2^V es un subconjunto de V, por lo que $|2^V| \leq |V|$. Se tiene así la fórmula insatisfactible $|V| < |2^V|$ y $|2^V| \leq |V|$, luego, por RAA, V no puede ser el conjunto de todos los conjuntos. ■

Observación 13.8.0.— Resultado que demostraremos por reducción al absurdo en el ejemplo 398 (pág. 769 de esta edición) usando el axioma del par y el axioma de regularidad.

§ 13.9 Una infinidad de conjuntos infinitos, I

En un más que breve resumen, en este punto, diríamos:

$$\aleph_0 = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|,$$
$$\aleph_0 < 2^{\aleph_0} = \mathfrak{c},$$
$$\mathfrak{c} = |\mathbb{R}| = |2^{\mathbb{N}}| = |2^{\mathbb{Z}}| = |2^{\mathbb{Q}}|.$$

El teorema de CANTOR permite afirmar la existencia de una infinidad de conjuntos infinitos,

$$\mathbb{N}, 2^{\mathbb{N}}, 2^{2^{\mathbb{N}}}, 2^{2^{2^{\mathbb{N}}}}, \ldots$$

[19] *Cfr. infra* teorema 13.31 (pág. 743 de esta edición).

y, por tanto, de una sucesión S_0, estrictamente creciente de cardinales infinitos,

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \cdots$$

sucesión, que comienza donde «termina» la de números cardinales finitos.

Ejemplo 395

A lo largo de la historia se ha dado nombre a algunos subconjuntos de números naturales, $\text{Enteros}^+ = \mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$, $\text{Pares}^+ = 2\mathbb{Z}^+ = \{2, 4, \ldots\}$, $\text{Impares}^+ = \mathbb{Z}^+ \setminus 2\mathbb{Z}^+ = \{1, 3, 5, \ldots\}$, etc. La cuestión es, ¿pudiésemos construir un algoritmo para asignar un nombre a todos los subconjuntos de números naturales?

Resolución.— Las lenguas naturales que hablamos y los lenguajes formales que utilizamos se basan en un alfabeto a lo sumo numerable y unas reglas de composición que determinan que la cantidad de frases posibles es numerable —una unión numerable de conjuntos finitos o numerables—. Por esto y debido al teorema de CANTOR, la respuesta es no. Como corolario, pensemos que es imposible igualmente proporcionar nombre a todos los números reales, a todos los subconjuntos de números reales, etc. ■

Observación 13.9.0.— La teoría de CANTOR de los números transfinitos no ha estado ni está exenta de polémica[20]; de hecho, de la oposición, surgió la escuela constructivista[21]y su rama intuicionista[22].

§ 13.10 Aritmética para $\aleph_0$ y $\mathfrak{c}$

La aritmética de los cardinales fue desarrollada por CANTOR (1887; 1895). Tenemos unas primeras reglas de cálculo para $\aleph_0$ y las operaciones $+$ y $\cdot$. Una forma intuitiva de sumar dos números naturales, n y m, es elegir un conjunto X de cardinal n y otro conjunto Y, de cardinal m, y definir $n + m$, como el cardinal de $X \cup Y$. Siguiendo esta línea, definimos también la multiplicación y la exponenciación.

Definición 13.11 (Operaciones con cardinales).— Sean $\mathfrak{x}$ e $\mathfrak{y}$ dos números cardinales, y X e Y dos conjuntos disjuntos de cardinalidades $\mathfrak{x}$ e $\mathfrak{y}$, respectivamente, entonces:

0. $\mathfrak{x} + \mathfrak{y} = |X \cup Y|$;

1. $\mathfrak{x} \cdot \mathfrak{y} = |X \times Y|$;

[20] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Controversy_over_Cantor's_theory.
[21] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Constructivism_(philosophy_of_mathematics).
[22] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Intuitionism.

2. $\mathfrak{x}^{\mathfrak{y}} = |X^Y|$.

El siguiente teorema permite demostrar que las operaciones anteriores están bien definidas[23].

Teorema 13.27 (Que relaciona las operaciones con la equipotencia)
Consideremos los conjuntos $X_0 \approx X_1$ e $Y_0 \approx Y_1$, entonces:

0. si $X_0 \cap Y_0 = X_1 \cap Y_1 = \emptyset$, entonces $X_0 \cup Y_0 \approx X_1 \cup Y_1$;
1. $X_0 \times Y_0 \approx X_1 \times Y_1$;
2. ${X_0}^{Y_0} \approx {X_1}^{Y_1}$.

Teorema 13.28 (Que destaca algunas propiedades de las operaciones entre cardinales)
Sean $\mathfrak{x}$, $\mathfrak{y}$ y $\mathfrak{z}$, tres números cardinales, entonces:

0. $\mathfrak{x} + \mathfrak{y} = \mathfrak{y} + \mathfrak{x}$;
1. $\mathfrak{x} \cdot \mathfrak{y} = \mathfrak{y} \cdot \mathfrak{x}$;
2. $(\mathfrak{x} + \mathfrak{y}) + \mathfrak{z} = \mathfrak{x} + (\mathfrak{y} + \mathfrak{z})$;
3. $(\mathfrak{x} \cdot \mathfrak{y}) \cdot \mathfrak{z} = \mathfrak{x} \cdot (\mathfrak{y} \cdot \mathfrak{z})$;
4. $\mathfrak{x}^{(\mathfrak{y}+\mathfrak{z})} = \mathfrak{x}^{\mathfrak{y}} \cdot \mathfrak{x}^{\mathfrak{z}}$;
5. $(\mathfrak{x} \cdot \mathfrak{y})^{\mathfrak{z}} = \mathfrak{x}^{\mathfrak{z}} \cdot \mathfrak{y}^{\mathfrak{z}}$;
6. $(\mathfrak{x}^{\mathfrak{y}})^{\mathfrak{z}} = \mathfrak{x}^{\mathfrak{y} \cdot \mathfrak{z}}$.

Teorema 13.29 (Operaciones y orden)
Sean $\mathfrak{x}$, $\mathfrak{y}$ y $\mathfrak{z}$, tres números cardinales, entonces:

0. $\mathfrak{x} \leq \mathfrak{y} \to \mathfrak{x} + \mathfrak{z} \leq \mathfrak{y} + \mathfrak{z}$;
1. $\mathfrak{x} \leq \mathfrak{y} \to \mathfrak{x} \cdot \mathfrak{z} \leq \mathfrak{y} \cdot \mathfrak{z}$;
2. $\mathfrak{x} \leq \mathfrak{y} \to \mathfrak{x}^{\mathfrak{z}} \leq \mathfrak{y}^{\mathfrak{z}}$;
3. $\mathfrak{x} \leq \mathfrak{y} \to \mathfrak{z}^{\mathfrak{x}} \leq \mathfrak{z}^{\mathfrak{y}}$, no siendo cero a la vez $\mathfrak{x}$ e $\mathfrak{y}$.

Teorema 13.30 (Algunas reglas de cálculo para $\aleph_0$)
$\forall n \in \mathbb{N}$:

0. $n + \aleph_0 = \aleph_0$;
1. $\aleph_0 + \aleph_0 = \aleph_0$;
2. si $n > 0$, $n \cdot \aleph_0 = \aleph_0$;
3. $\aleph_0 \cdot \aleph_0 = \aleph_0$;
4. si $n > 0$, ${\aleph_0}^n = \aleph_0$.

[23] *Cfr. infra* actividad 13.7 (pág. 748 de esta edición).

Actividad 13.2

Demostremos el teorema anterior.

Indicaciones:

0. no es difícil a partir de saber que la unión de un conjunto finito y un conjunto numerable es numerable (*cfr. supra* teorema 13.12 [pág. 731 de esta edición]);
1. no es difícil a partir de saber que la unión finita de dos conjuntos numerables es numerable (caso particular del teorema 13.14 [pág. 731 de esta edición]);
2. no es difícil a partir de saber que la unión finita de conjuntos numerables es numerable (*cfr. supra* teorema 13.14 [pág. 731 de esta edición]);
3. no es difícil a partir de saber que la unión numerable de conjuntos numerables es numerable (*cfr. supra* teorema 13.16 [pág. 732 de esta edición]) o que el producto cartesiano finito de conjuntos numerables es numerable (*cfr. supra* teorema 13.17 [pág. 734 de esta edición]);
4. no es difícil a partir de saber que el producto cartesiano finito de conjuntos numerables es numerable (*cfr. supra* teorema 13.17 [pág. 734 de esta edición]).

Teorema 13.31 (Algunas reglas de cálculo para $\aleph_0$ y $\mathfrak{c}$)

$\forall n \in \mathbb{N}$:

0. $\mathfrak{c} + \mathfrak{c} = \mathfrak{c}$;
1. $n > 0 \to n \cdot \mathfrak{c} = \mathfrak{c}$;
2. $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$;
3. $n > 0 \to \mathfrak{c}^n = \mathfrak{c}$;
4. $\aleph_0 \cdot \mathfrak{c} = \mathfrak{c} \cdot \aleph_0 = \mathfrak{c}$;
5. $n^{\aleph_0} = \mathfrak{c}$;
6. $\aleph_0^{\aleph_0} = \mathfrak{c}$;
7. $2 \leq n < \aleph_0 \to \mathfrak{c}^{\aleph_0} = \mathfrak{c}$;
8. $n^{\mathfrak{c}} = 2^{\mathfrak{c}}$;
9. ${\aleph_0}^{\mathfrak{c}} = 2^{\mathfrak{c}}$;
10. $\mathfrak{c}^{\mathfrak{c}} = 2^{\mathfrak{c}}$;
11. $(2^{\mathfrak{c}})^{\mathfrak{c}} = 2^{\mathfrak{c}}$;
12. $\aleph_0 < 2^{\aleph_0}$;
13. $\mathfrak{c} < 2^{\mathfrak{c}}$.

Observación 13.10.0.— Es interesante reflexionar sobre lo que nos dicen algunas de estas reglas; a modo de ejemplo:

0. $\mathfrak{c}^n = \mathfrak{c}$ $(n \in \mathbb{Z}^+)$ expresa que el *número de puntos del espacio n dimensional* es el mismo que el de una recta;

1. en particular ($n = 2$), $\mathfrak{c}^2 = \mathfrak{c}$ expresa que el *número de puntos de un plano es el mismo que el de una recta*;

2. $\mathfrak{c} < 2^{\mathfrak{c}}$ expresa que *existen más funciones reales de variable real que números reales*.

Observación 13.10.1.— Finalmente notemos que algunas reglas válidas para cardinales finitos no lo son para cardinales infinitos, por ejemplo, la regla «si $\mathfrak{x} < \mathfrak{y}$ y $\mathfrak{z} \neq 0$ entonces $\mathfrak{x}^{\mathfrak{z}} < \mathfrak{y}^{\mathfrak{z}}$» no es válida; un contraejemplo para ésta: si $\mathfrak{x} = \aleph_0$, $\mathfrak{x} = \mathfrak{c}$ y $\mathfrak{z} = \aleph_0$,entonces $\aleph_0 < \mathfrak{c}$ y $\aleph_0 \neq 0$, y sin embargo, $\aleph_0^{\aleph_0} = \mathfrak{c} \not< \mathfrak{c} = \mathfrak{c}^{\aleph_0}$.

§ 13.11 Acerca de la sucesión de infinitos

Ya observamos que el teorema de Cantor[24] permite afirmar la existencia de una infinidad de conjuntos infinitos,

$$\mathbb{N} \prec 2^{\mathbb{N}} \prec 2^{2^{\mathbb{N}}} \prec 2^{2^{2^{\mathbb{N}}}} \prec \dots$$

y, por tanto, de una sucesión estrictamente creciente $\mathfrak{S}_0$ de cardinales infinitos,

$$\aleph_0 < 2^{\aleph_0} < 2^{2^{\aleph_0}} < \dots$$

Sucesiones que es posible identificar con clases, a saber, la clase de los cardinales finitos y la clase $\mathfrak{C}_0$ de los cardinales infinitos álefs.

Observemos que operando con un número finito de cardinales finitos —términos de la sucesión $0, 1, 2, \dots$—, con las operaciones habituales de suma y multiplicación, nunca obtendremos $\aleph_0$ como resultado. Decimos que la clase $\mathfrak{C}_0$ es inalcanzable desde la clase de los cardinales finitos.

Esta idea la trasladó Gödel hacia cardinales mayores. Si pensamos en la unión de conjuntos cualesquiera con cardinales de $\mathfrak{C}_0$, entonces el cardinal de esta unión, al que designaremos por Ω_0, es mayor que cualquiera de los cardinales $\aleph_0, 2^{\aleph_0}, 2^{2^{\aleph_0}}, \dots$, es inalcanzable. Así, tenemos otra sucesión estrictamente creciente, $\mathfrak{S}_1$,

$$\Omega_0 < 2^{\Omega_0} < 2^{2^{\Omega_0}} < \dots$$

y su correspondiente clase $\mathfrak{C}_1$, la clase de los cardinales infinitos inalcanzables desde la clase $\mathfrak{C}_0$.

Si consideremos ahora la unión de conjuntos cualesquiera con cardinales de $\mathfrak{C}_0$ y de de $\mathfrak{C}_1$, entonces el cardinal de esta unión, al que llamamos Ω_1, es mayor que cualquiera de los cardinales obtenidos anteriormente, obteniéndose una nueva sucesión, $\mathfrak{S}_2$, estrictamente creciente,

$$\Omega_1 < 2^{\Omega_1} < 2^{2^{\Omega_1}} < \dots$$

y su correspondiente clase $\mathfrak{C}_2$, la clase de los cardinales infinitos inalcanzables desde la clase $\mathfrak{C}_1$ o $\mathfrak{C}_0$.

[24] *Cfr. supra* teorema 13.26 (pág. 739 de esta edición).

Seguiría la clase de los cardinales inalcanzables desde las clases anteriores y así sucesivamente. Generando nuevos cardinales de esta forma, vemos que tenemos la siguiente sucesión estrictamente creciente $\mathfrak{C}$ de cardinales infinitos:

$$\aleph_0, 2^{\aleph_0}, 2^{2^{\aleph_0}}, \ldots, \Omega_0, 2^{\Omega_0}, 2^{2^{\Omega_0}}, \ldots, \Omega_1, 2^{\Omega_1}, 2^{2^{\Omega_1}}, \ldots, \Omega_2, 2^{\Omega_2}, 2^{2^{\Omega_2}}, \ldots$$

Teorema 13.32

La sucesión $\mathfrak{C}$ satisface las siguientes propiedades:

0. $\mathfrak{C}$ es una sucesión estrictamente creciente;
1. dado un conjunto cualquiera de números cardinales de $\mathfrak{C}$, existe en $\mathfrak{C}$ un número cardinal que los supera a todos y que es precisamente el menor de los números cardinales en $\mathfrak{C}$ que los supera a todos;
2. $\mathfrak{C}$ es infinita en un sentido mucho más amplio; con esto queremos decir que no es posible considerar el conjunto de todos sus elementos sin incurrir en una paradoja, la antinomia de Cantor (*cfr. infra* teorema 14.10.2 [pág. 780 de esta edición]).

A lo largo de los años, en el estudio de la jerarquía de grandes cardinales se han definido varias clases de cardinales: *medibles*, *fuertes*, *superfuertes*, *supercompactos*, *extensibles*, *inmensos*, etc.[25]

Hipercomputabilidad

Pudiésemos decir que una máquina de Turing está en el orden de $\aleph_0$, con una cinta infinita con un número infinito numerable de registros que podemos recorrer con un cabezal de lectoescritura. Desconocemos cómo hacer este recorrido en los órdenes siguiente: por ejemplo, justo en el siguiente, $2^{\aleph_0}$, esto es, $\mathfrak{c}$, habría tantos registros en la cinta como números reales, y en el siguiente a éste, $2^{\mathfrak{c}}$, tantos como funciones reales de variable real. ¿Cómo dirigir el cabezal de lectoescritura al «siguiente» a un registro dado? ¿Existe tal posibilidad? Bien que admitir el axioma de elección es admitir que en todo conjunto puede definirse un orden bueno[*], pero...

Sin más divagaciones, la situación actual es que ningún computador, supercomputador, computador cuántico[†] o red o sistema de cualesquiera de ellos dispone de una fuente inagotable a demanda de memoria (una cinta de registros infinitamente extensible), por lo que pudiésemos decir que un computador actual (la plasmación física actualmente posible de una máquina de Turing) está en un orden finito, infinitamente lejos de $\aleph_0$, el orden de una máquina de Turing.

Volviendo al comienzo de este apunte, ¿pudiésemos imaginar lo que sería una computabilidad en los órdenes $2^{\aleph_0}, 2^{2^{\aleph_0}}, \ldots, \Omega_0, 2^{\Omega_0}, 2^{2^{\Omega_0}}, \ldots, \Omega_1, 2^{\Omega_1}, 2^{2^{\Omega_1}}, \ldots, \Omega_2, 2^{\Omega_2},$

[25] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Large_cardinal y https://en.wikipedia.org/wiki/List_of_large_cardinal_properties.

$2^{2^{\Omega_2}}, \ldots$? ¿Y una computabilidad práctica, no sólo teórica, en estos diferentes órdenes de hipercomputación*?

---

* *Vid. infra* teorema 14.11 (pág. 765 de esta edición).
† Un computador cuántico actual también es una plasmación física posible de la máquina de Turing que va a resolver exactamente los mismos problemas que los computadores no cuánticos, sólo que, en principio, mucho más rápidamente.
* *Cfr. v. gr.* https://en.wikipedia.org/wiki/Hypercomputation.

§ 13.12 Muestra de más ejemplos

Ejemplo 396

Sea C un conjunto y $x \notin C$. Demostremos que si C es infinito numerable, entonces, $C \cup \{x\}$ también lo es.

[Cubit 83], [SEL 5.2]. *Cfr.* Anzola y Caruncho [140]: problema 7.52 (pág. 168).

Resolución.— Por definición de conjunto numerable, como C lo es, existe una biyección $f : \mathbb{N} \longrightarrow C$. Sea $g : \mathbb{N} \longrightarrow C \cup \{x\}$, definida por $g(n) = x$, si $n = 0$ y por $g(n) = f(n-1)$, si $n \neq 0$, esto es, la correspondencia g se define en dos subdominios, en $\{0\}$ como la correspondencia constante x, aplicación biyectiva, y en $\mathbb{Z}^+$ como f, también biyectiva, y como dichos subdominios son disjuntos y sus imágenes, C y $\{x\}$, también, se tiene que g es biyectiva. ■

Ejemplo 397

Usando el lema diagonal de Cantor, demostremos por reducción al absurdo que el conjunto potencia de $\mathbb{N}$ no es numerable.

[Cubit 86].

Resolución.— Razonemos por reducción al absurdo. Supongamos que $2^{\mathbb{N}}$ es numerable. y plasmemos esto en que exista una enumeración de todos los subconjuntos de $\mathbb{N}$, que denotamos como $\{P_0, P_1, P_2, \ldots\}$.

A modo de ejemplo, supongamos que los primeros subconjuntos de de dicha enumeración fuesen $P_0 = \{1, 2\}$, $P_1 = \{1, 3, 5\}$, $P_2 = \{0, 2, 4\}$ y $P_3 = \emptyset$:

m	0	1	2	3	...
P_0	$\boxed{0}$	1	1	0	...
P_1	0	$\boxed{1}$	0	1	...
P_2	1	0	$\boxed{1}$	0	...
P_3	0	0	0	$\boxed{0}$	...
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Podemos definir la enumeración $\{P_0, P_1, P_2, \dots\}$ mediante una relación diádica $P(n, m)$ que indique si $m \in P_n$; por facilidad, notamos $P(n, m)$ por $P_n(m)$; así, $P_n(m) \leftrightarrow m \in P_n$.

Sea Q tal que $(\forall n \in \mathbb{N})(Q(n) \leftrightarrow \neg P(n, n))$, esto es, $n \in Q \leftrightarrow \neg P_n(n)$, es decir, $Q = \{n \in \mathbb{N} : n \notin P_n)\}$.

Percibimos esto en el ejemplo: $0 \in Q \leftrightarrow 0 \notin P_0$, $1 \in Q \leftrightarrow 1 \notin P_1$, $2 \in Q \leftrightarrow 2 \notin P_2$, $3 \in Q \leftrightarrow 3 \notin P_3$, por lo que $Q = \{0, 3, \dots\}$.

Del lema diagonal de Cantor, deducimos que $\forall n \in \mathbb{N}$, $P_n \neq Q$.

Apreciamos esta conclusión en el ejemplo: Q difiere de P_0 ($0 \in Q$ y $0 \notin P_0$), Q difiere de P_1 ($1 \notin Q$ y $1 \in P_1$), Q difiere de P_2 ($1 \notin Q$ y $1 \in P_2$), Q difiere de P_3 ($3 \in Q$ y $3 \notin P_3$), y así sucesivamente.

Por reducción al absurdo, deducimos que $2^{\mathbb{N}}$ no es numerable. ■

§ 13.13 Propuesta de más actividades

Actividad 13.3

Sea A un alfabeto, α una palabra y ϵ la palabra vacía. Demostremos por inducción la equivalencia de las dos definiciones siguientes, Def_0 y Def_1, de palabra palíndroma. Notemos por $/$ al conjunto de palabras palíndromas del alfabeto A:

- Def_0: $(\forall \alpha, \alpha = a_0 a_1 \dots a_n)\,(\alpha \in / \leftrightarrow a_0 a_1 \dots a_n = a_n \dots a_1 a_0)$.
- Def_1: (definición inductiva)
  $\epsilon \in / \land \text{long}\ \alpha = 1 \to \alpha \in / \land (\forall a \in A)(\forall \alpha \in /)(a \alpha a \in /)$.

Actividad 13.4

Demostremos el teorema 13.2 (pág. 719 de esta edición).

Actividad 13.5

Demostremos que si $X \setminus Y$ es equipotente a $Y \setminus X$, entonces X es equipotente a Y.

[Cubit 90].

Con miras a su resolución.— Como $X \setminus Y$ es equipotente a $Y \setminus X$, existe una biyección de $X \setminus Y$ en $Y \setminus X$; todo consiste en auxiliarnos de tal biyección para definir una biyección de X en Y según los orígenes sean o no elementos de Y.

Actividad 13.6

En sus *Principia Mathematica* (1912), Russell y Whitehead definen conjunto finito de la siguiente forma:

> Dados un conjunto a, y $u \subseteq Pa$, decimos que u es una familia inductiva de conjuntos de a si, y sólo si, $\emptyset \in u$ y para todo $x \in u$ e $y \in a$, también ocurre que $x \cup \{y\} \in u$, entonces, a es un conjunto finito, si, y sólo si, pertenece a cualquier familia inductiva de subconjuntos suyos. Si no es finito, decimos que es un conjunto infinito.

¿Coincide ésta con las definiciones vistas de Tarski, Cantor y Dedekind (*cfr. supra* § 13.3.0 [pág. 722 de esta edición])?

Actividad 13.7

Demostremos que las operaciones entre cardinales, suma, producto y exponenciación estudiadas en la definición 13.11 (pág. 741 de esta edición) están bien definidas.

Sugerencia.— Es posible una demostración usando la actividad 10.12 (pág. 570 de esta edición) y el teorema 13.27 (pág. 742 de esta edición).

Actividad 13.8

Demostremos que si C es un conjunto infinito numerable, entonces C tiene subconjuntos propios infinitos numerables.

[Cubit 84], [SEL 5:1]. *Cfr.* Anzola y Caruncho [140]: problema 7.26 (pág. 155).

Actividad 13.9

Demostremos que el conjunto de todas las palabras binarias de longitud finita es numerable.

[Cubit 87].

Con miras a su resolución.— Siendo $\Sigma = \{0, 1\}$, precisamente es Σ^*, su clausura de Kleene[26], el conjunto de interés. Por su definición inductiva[27], Σ^* es una unión numerable de conjuntos finitos, la cual es numerable [por el teorema 13.15 (pág. 732 de esta edición)].

---

[26] *Vid. supra* pág. lxxxv.
[27] *Vid. supra* pág. lxxxvi.

Actividad 13.10

Demostremos que el conjunto de todos los subconjuntos finitos de números naturales es numerable.

Sugerencia.— Es posible encontrar una codificación de tales conjuntos como palabras binarias de longitud finita.

[Cubit 88].

Con miras a su resolución.— Utilizamos una codificación de ausencia (0) y presencia (1) con referente el conjunto de números naturales $\mathbb{N}$; por ejemplo, la codificación de $\{2, 5, 7, 11\}$ es 001001010001 —codificación que anticipamos en el ejemplo 54 (pág. 47 de esta edición)—. Dicho de otro modo, cada subconjunto finito de naturales corresponde a una palabra binaria de longitud finita. Hemos definido así una inyección —las codificaciones de dos subconjuntos distintos son distintas— del conjunto de todos los subconjuntos finitos de números naturales en el conjunto de todas las palabras binarias de longitud finita. Como éste es numerable [por Cubit 87], se sigue que aquél también lo es [por el teorema 13.11 (pág. 731 de esta edición)].

Actividad 13.11

Consideremos un alfabeto infinito numerable; demostremos que todos y cada uno de los siguientes conjuntos son numerables:

0. palabras de dos letras;
1. palabras de tres letras;
2. dado $n \in \mathbb{N}_{>3}$, palabras de n letras;
3. todas las palabras de longitud finita.

[Cubit 89].

Con miras a su resolución.— En efecto; sea Σ el mencionado alfabeto infinito numerable, entonces:

0. el conjunto de palabras de dos letras de Σ es el producto cartesiano $\Sigma \times \Sigma$, abreviadamente, Σ^2, que por el teorema 13.17 (pág. 734 de esta edición) es numerable;

1. el conjunto de palabras de tres letras de Σ es el producto cartesiano $\Sigma \times \Sigma \times \Sigma$, abreviadamente, Σ^3, que por el teorema 13.17 (pág. 734 de esta edición) es numerable;

2. el conjunto de palabras de n letras de Σ (con $n \in \mathbb{N}_{>3}$) es el producto cartesiano Σ^n que por el teorema 13.17 (pág. 734 de esta edición) es numerable;

3. el conjunto Σ^* de todas las palabras con un número finito de letras de Σ se define inductivamente:
   0. $\Sigma^0 = \{\varepsilon\}$; (conjunto de las palabras de longitud 0)
   1. $\Sigma^1 = \Sigma$; (conjunto de las palabras de longitud 1)
   2. $\Sigma^i = \Sigma^{i-1} \times \Sigma$ (para $2 \leq i$); (conjunto de las palabras de longitud i)
   3. $\Sigma^* = \Sigma^0 \cup \bigcup_{i \in \mathbb{Z}^+} \Sigma^i$; (conjunto de las palabras de longitud finita)

ahora bien, como Σ^0 es finito y $\bigcup_{i\in\mathbb{Z}^+}\Sigma^i$ es una unión numerable de conjuntos numerables —$\forall i\in\mathbb{Z}^+$, Σ^i es numerable [por los apartados anteriores]— y, por tanto, numerable [por el teorema 13.16 (p. 732 de esta edición)], su unión, Σ^*, es numerable [por el teorema 13.12 (p. 731 de esta edición)].

Actividad 13.12

Demostremos que si X es numerable, entonces existe un subconjunto Y numerable de X tal que $X\setminus Y$ es numerable.

[Cubit 91].

Con miras a su resolución.— Como X es numerable, existe $f:\mathbb{N}\to X$ biyectiva; tomamos como Y la imagen por f de un subconjunto numerable C de $\mathbb{N}$ tal que $\mathbb{N}\setminus C$ sea también numerable (por ejemplo, $C=$ Pares no negativos).

Actividad 13.13

Demostremos que el conjunto de todas las aplicaciones de $\mathbb{N}$ en $\mathbb{N}$ no es numerable.

§ 13.14 Bibliografía

- Para leer:

[182] Francesc Rossell i Pujós. *El infinito. ¿Es un viaje o un destino?* Grandes ideas de las matemáticas. EMSE EDAPP y Prisanoticias Colecciones, Barcelona, Cataluña (ES-CT), España, 2019.

- Para estudiar y practicar:

[147] Herbert Bruce Enderton. *Elements of Set Theory*. Academic Press, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1977.

[148] Karel Hrbacek y Thomas J. Jech. *Introduction to set theory*. Monographs and textbooks in pure and applied mathematics. Marcel Dekker, Nueva York, Nueva York (US-NY), Estados Unidos de América, 3.ª ed., 1999.

[183] Julián Garrido Garrido. *Verdad matemática: introducción a los fundamentos de la matemática*. Ciencia abierta. Nivola, Madrid, Comunidad de Madrid (ES-M), España, 2003.

[140] Máximo Anzola González y José Ramón Caruncho Castro. *Problemas de álgebra. Tomo 1: Conjuntos - Grupos*. Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1981. ©TDR.

- Para profundizar, acullá:

[142] José Antonio Alonso Jiménez, Joaquín Borrego Díaz, Mario de Jesús Pérez Jiménez y José Luis Ruiz Reina. *Curso Práctico de Teoría de Conjuntos*. La Ñ, Sevilla, Andalucía (ES-AN), España, 1998.

CAPÍTULO 14

Lógica de conjuntos: primeras axiomáticas

Saber algo bien y a fondo deja más huella que pretender saberlo todo y todo por igual.
(Norberto CUESTA DUTARI).

Los axiomas hacen el papel de principios, inmutables, piezas indeformables con las que construir sistemas. Los axiomas deben reflejar nuestro conocimiento informal de dicho sistema, en este caso de los conjuntos.

Recordemos el *desideratum* del programa de HILBERT para los sistemas axiomáticos:

Formalización.— La axiomática se presentará formalizada con fórmulas lógicas.
Independencia.— Ningún axioma deberá ser demostrable a partir de los otros del sistema.
Completitud.— En un sistema axiomático debe poder ser demostrada/derivada cualquier fórmula válida a partir de los axiomas.
Consistencia.— No pueden demostrarse/derivarse en el mismo sistema axiomático una fórmula y su negación.
Decidibilidad.— Debe existir un procedimiento que permita conocer si una fórmula dada es demostrable/derivable en el sistema.
Categoricidad.— Todos los modelos que satisfagan la totalidad de los axiomas deben ser isomorfos entre sí.

§ 14.0 Axiomas de extensionalidad y comprensión

Como ya dijimos, la idea de Cantor de lo que es un conjunto: «cualquier colección en un todo M de objetos definidos y separados, proporcionada por nuestra intuición o nuestro pensamiento» —por cierto, que es la idea natural que posee cualquiera no versado en Matemáticas— es errónea, desde el momento que conduce a paradojas, como la de Russell: «si la colección de todos los conjuntos que no son elementos de sí mismos fuese un conjunto, entonces, para este conjunto, la propiedad de ser un elemento de sí mismo equivale a no serlo».

Russell y Whitehead resolvieron este problema en sus *Principia Mathematica* (1910), estableciendo una teoría de tipos de colecciones: una colección x puede ser miembro de una colección y, sólo si y está situada un escalón más arriba en la jerarquía de colecciones en la que está x. Este sistema tiene infinitas nociones primitivas. Las axiomáticas de Zermelo, Fraenkel y Skolem (ZFS), con dos nociones primitivas: las de conjunto y pertenencia, y la de John von Neumann, Bernays y Gödel (NBG), con tres: conjunto, clase y pertenencia, se han convertido en clásicas, siendo la elección entre ellas una cuestión casi de preferencias. Ambos sistemas son básicamente equivalentes: todo axioma de ZFS es un teorema en NBG, por lo que la consistencia de NBG implica la de ZFS; además, toda fórmula cerrada (sin variables libres) de ZFS que sea un teorema en NBG, lo es en ZFS, de donde la consistencia de ZFS implica la de NBG —*cfr.* Alonso Jiménez, Borrego Díaz, Pérez Jiménez y Ruiz Reina [142] (pág. xxi).

Es posible consultar cualquiera de ambas axiomáticas en variadas fuentes, por ejemplo: Alonso Jiménez, Borrego Díaz, Pérez Jiménez y Ruiz Reina [142]; Levy [184]; Devlin [185]; Takeuti y Zaring [186].

§ 14.1 Axiomas F (F de Frege)

Recordemos cuando en la *teoría ingenua de conjuntos*° hemos estudiado las primeras nociones sobre conjuntos y aprendimos sobre cómo *definir un conjunto por extensión* (listando todos sus elementos), *o por comprensión* (proporcionando una propiedad característica común a todos los elementos del conjunto).

° Puede que sea ingenua por inconsistente como la propuesta por Friedrich Ludwig Gottlob Frege que vemos en aquí o, aun siendo consistente, por la propia presentación de la teoría como en el caso de Paul Richard Halmos [187] —*cfr. v. gr.* https://en.wikipedia.org/wiki/Naive_set_theory

La formalización de ambas ideas aparece en FREGE (1893), en un primer intento de proporcionar una axiomática para la teoría de conjuntos. La primera idea, el hecho de que un conjunto esté determinado de manera única por los elementos que lo forman, se recoge en el siguiente axioma, que permite decidir si dos conjuntos son o no, iguales.

§ 14.1.0 Axioma de extensionalidad

Axioma de Extensionalidad (AE)

(FREGE, 1893; versión de RUSSELL de 1903). Dos conjuntos son idénticos si tienen los mismos elementos. En signos lógico-matemáticos,

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \to x = y).$$

El recíproco también es verdadero: si dos conjuntos son iguales, entonces, tienen los mismos elementos.

$$\forall x \forall y (x = y \to \forall z (z \in x \leftrightarrow z \in y)). \tag{14.0}$$

Pero no sólo queremos decidir la igualdad de conjuntos, sino que también deseamos encontrarlos o saber cómo construirlos. ¿Será cierto que cualquier colección de objetos, por ejemplo, conjuntos, es un conjunto? Parece que lo único que debemos exigir es que cualquier colección de conjuntos, a la que queramos llamar conjunto, deba poder especificarse en nuestro lenguaje de la teoría de conjuntos, y la situación ideal sería que, para toda afirmación (fórmula) formulada en tal lenguaje, ϕ, fuese un conjunto, la colección de todos los conjuntos que la verifican, $\{x : \phi(x)\}$. No estamos diciendo que debamos exigir que todos los conjuntos deban ser especificables; de hecho, el axioma de elección[1] implicará la existencia de conjuntos no necesariamente especificables. Lo que decíamos es que todas las colecciones especificables deben ser conjuntos, lo cual se recoge en el siguiente axioma, en realidad, un esquema de axiomas.

§ 14.1.1 Esquema de axiomas de comprensión

Esquema de axiomas de comprensión

(FREGE, 1893; versión de RUSSELL de 1903). Para cualquier propiedad ϕ existe un conjunto al que pertenecen todas y sólo esas entidades para las que ϕ es verdadera. Es posible hacer de cualquier propiedad la condición definidora de un conjunto. En signos lógico-matemáticos,

$$\exists y \forall x (x \in y \leftrightarrow \phi(x)).$$

Es un *esquema de axioma*, esto es, un colección infinita de axiomas, que se genera permitiendo que $\phi(x)$ pueda ser cualquier fórmula, del lenguaje de la teoría de conjuntos, en la que la variable

[1] *Cfr. infra* § 14.3.0 (pág. 763 de esta edición).

y no sea libre. Para cada ϕ particular, se tiene un «axioma de comprensión» (también llamado una *instancia* del esquema). Si bien, en general, también nos referiremos a este esquema simplemente como axioma de comprensión.

§ 14.1.2 La antinomia de RUSSELL

Pero el axioma de comprensión no es consistente. Justo cuando FREGE iba a publicar sus *Grundgesetze der Arithmetik*, donde pretendía reconstrur la aritmética a partir de la teoría de conjuntos, recibió una carta de RUSSELL, en la que éste le mostraba un grave problema de fundamentos, referido a la autopertenencia de conjuntos.

> CANTOR tenía una prueba de que no existe el número más grande, y a mí me parecía que el número de todas las cosas del mundo debería ser el más grande posible. Consiguientemente examiné su prueba con detalle, y me propuse aplicarlo a la categoría de todas las cosas que existen. Esto me llevó a considerar aquellas categorías que no son miembros de sí mismas, y a preguntarme si la categoría de tales categorías es o no miembro de sí misma. Encontré que cualquier respuesta implica la contraria.
>
> (Bertrand Arthur William RUSSELL).

Es posible clasificar todos los conjuntos en dos clases. Algunos conjuntos satisfacen la propiedad que los define (por ejemplo, «el conjunto de todos los objetos describibles en exactamente trece palabras castellanas»), o sea, son conjuntos que se contienen a sí mismos como elementos. Llamémoslos conjuntos autocontenidos (tipo A). El conjunto de todos los zapatos no es un zapato, por lo que sería un conjunto no autocontenido (tipo $\neg A$). Argumentaba RUSSELL: sea B la colección de todos los conjuntos no autocontenidos (lo cual es una colección especificable en nuestro lenguaje de conjuntos), si B es un conjunto, entonces es un conjunto A o un conjunto $\neg A$. Si B es de tipo A, entonces, por definición de B, B no se autocontiene, o sea, es un conjunto $\neg A$, así que, B no es un conjunto o $A \cap (\neg A) \neq \emptyset$. Si B es $\neg A$, entonces, por definición de B, B debe autocontenerse, esto es, B es un conjunto A, de donde, B no es un conjunto o $A \cap (\neg A) \neq \emptyset$. Como, claramente, $A \cap (\neg A) = \emptyset$, se deduce que B no puede ser un conjunto, por lo que no toda colección especificable en nuestro lenguaje de conjuntos es un conjunto.

> Un científico apenas puede encontrarse con algo más indeseable que el ver cómo el fundamento de su obra se desploma precisamente cuanto la obra está acabada. Yo he sido puesto en esta situación por una carta del señor Bertrand RUSSELL, cuando la obra estaba ya a punto de salir de la prensa.
>
> (Friedrich Ludwig Gottlob FREGE).

Cuando FREGE comenzó a recibir las pruebas de imprenta de su libro, suprimió páginas enteras. Finalmente, añadió dos apéndices a su libro, en el primero describía sus propias opiniones, y en el segundo, aportaba un método algo rudimentario y elemental para evitar la paradoja.

Teorema 14.0 (Antinomia de RUSSELL, 1903)
$\neg\exists y\forall x(x \in y \leftrightarrow x \notin x)$.

Demostración.— En efecto, supongamos que y es un conjunto tal que $\forall x(x \in y \leftrightarrow x \notin x)$, entonces, en particular, para el conjunto y (esto es, cuando x es y), se tiene $y \in y \leftrightarrow y \notin y$, lo cual es una fórmula insatisfactible. ■

Es costumbre, en teoría de conjuntos, llamar *antinomia*, a cualquier refutación de alguna instancia del axioma de comprensión. Resulta que la *antinomia de* RUSSELL es la más sencilla.

Según RUSSELL, debido al principio del tercio excluido, una colección C, bien se contiene a sí misma como elemento, bien no se contiene a sí misma como elemento. Por el axioma de comprensión, si $\phi x \risingdotseq$ x no se contiene a sí misma como elemento —esto es, $\phi x \risingdotseq x \notin x$—, entonces $\{x : \phi x\}(= \{x : x \notin x\})$ es el conjunto definido por ϕx. Consideremos la colección C como el conjunto $\{x : x \notin x\}$. En este caso, si C se contiene a sí mismo como elemento, $C \in C$, entonces, por definición de C, $C \notin C$ y, por otro lado, si $C \notin C$, entonces, por definición de C, $C \in C$. Actualmente, nos referimos a C como la clase de RUSSELL.

Algunas variantes de la antinomia de RUSSELL aparecen en la actividad 14.3 (pág. 782 de esta edición). Aunque la antinomia de RUSSELL, fue la primera, de una manera explícita, no lo fue, implícitamente, pues CANTOR en 1895 y BURALI-FORTI en 1897, descubrieron la, ahora conocida como, *paradoja de* BURALI-FORTI[2].

Observación 14.1.0.— Dada una fórmula ϕ, ¿existe un conjunto y tal que $\forall x(x \in y \leftrightarrow \phi(x))$? Puede que sí, pero nadie lo ha demostrado, para cualquier ϕ. Lo que sí es cierto, es que si tal y existe, entonces es único, debido a la transitividad de $\leftrightarrow$ y al axioma de extensionalidad.

§ 14.2 Axiomas Z (Z de ZERMELO)

Los axiomas siguen siendo de dos tipos, axiomas simples o esquemas de axiomas, como los estudiados de extensionalidad y de comprensión, respectivamente.

ZERMELO conserva el *axioma de extensionalidad*, pero abandona el axioma de comprensión si bien propone dos instancias de este último, el *axioma de unión* y el *axioma del conjunto potencia*. Recordemos[3] que el axioma de extensionalidad permite demostrar que cualquier conjunto cuya existencia sea propugnada por cualquier otro axioma es único, de ahí que podamos designarlos: conjunto vacío, par no ordenado, etc.

CANTOR proporciona versiones informales de los axiomas que indicamos.

[2] *Vid. infra* teorema 14.26 (pág. 780 de esta edición).
[3] *Cfr. supra* observación 14.1.0 (pág. 756 de esta edición).

El sistema axiomático Z está definido por los siguientes axiomas:

- axioma de extensionalidad (AE);
- axioma del conjunto vacío (AV);
- axioma de separación (AS) (esquema de axiomas);
- axioma de emparejamiento (AJ);
- axioma de la unión (AU);
- axioma del conjunto potencia (AP);
- axioma del infinito (AI).

§ 14.2.0 Axioma del conjunto vacío

Axioma del conjunto vacío (AV)

(Zermelo, 1908). Existe un conjunto sin elementos. Se nota $\emptyset$. En signos lógico-matemáticos,

$$\exists x \forall y \neg (y \in x).$$

Establece así Zermelo como axioma este punto de partida, a saber, la existencia de un conjunto para definir nuevos conjuntos a partir de él[4].

§ 14.2.1 Esquema de axiomas de separación

Esquema de axiomas de separación (AS) (o de especificación, o de subconjuntos)

(Cantor, 1899; Zermelo, 1908). Todo subconjunto definible a partir de un conjunto es un conjunto. En lenguaje lógico-matemático, dados un conjunto z y una propiedad $\phi(x)$, existe al menos un conjunto cuyos elementos son, y sólo son, los que satisfacen $\phi(x)$. En signos lógico-matemáticos,

$$\forall z \exists y \forall x (x \in y \leftrightarrow x \in z \wedge \phi(x)).$$

En definitiva, que $\{x \in z : \phi(x)\}$ es un conjunto.

Observación 14.2.0.— «Separamos» de z sus elementos que satisfacen ϕ; destacamos dicho subconjunto de z.

[4] Notemos que el conjunto vacío ya había sido definido por George Boole (1847, 1854) como aquel conjunto que no tiene elementos.

Es una especificación de la definición de Cantor de conjunto a partir de la satisfacción de propiedades; especifica que restringidas a conjuntos, las propiedades generan conjuntos, evitando así la paradoja de Russell, y que los conjuntos definidos a partir de propiedades son subconjuntos de conjuntos ya existentes —de aquí el nombre de «axiomas de subconjuntos»—, implicando, en particular, que $\mathcal{U}$ *no es un conjunto*.

Teorema 14.1
Si existe algún conjunto, el esquema de axiomas de especificación implica el axioma del conjunto vacío.

Demostración.— Sea z un conjunto y $\phi x \leftrightharpoons (x \neq x)$, de acuerdo con el esquema de axiomas de especificación, existe el conjunto y, subconjunto de z, formado por los x de z que satisfacen ϕ. Este y es un conjunto sin elementos. ∎

Teorema 14.2
La intersección de dos conjuntos es un conjunto.

Demostración.— Sean u y v conjuntos y sea $\phi(x, v) \leftrightharpoons x \in v$, entonces por el esquema de axiomas de especificación, dado u, existe y tal que para todo x, $x \in y$ si, y sólo si, $x \in u \wedge \phi(x, v)$. El nuevo conjunto y es el conjunto intersección de u y v. ∎

Teorema 14.3
La diferencia de dos conjuntos es un conjunto.

Demostración.— Sean u y v conjuntos y sea $\phi(x, v) \leftrightharpoons x \notin v$, entonces por el esquema de axiomas de separación, dado u, existe y tal que para todo x, $x \in y$ si, y sólo si, $x \in u \wedge \phi(x, v)$. El nuevo conjunto y es el conjunto diferencia $u \setminus v$. ∎

De este último teorema, el nombre de «axiomas de separación»: es posible separar los elementos de u en dos subconjuntos, según no sean de v o puedan serlo.

Observación 14.2.1.— Dos apuntes a destacar son los siguientes.

0. En este punto, con los axiomas de extensionalidad, del vacío y de separación, lo único que tenemos asegurado es que existe el conjunto vacío.

1. Que el de separación sea un esquema de axiomas significa que el número de axiomas del sistema Z es infinito.

§ 14.2.2 Axioma de emparejamiento

Axioma de emparejamiento (AJ)

(*Axioma del par* [o, sinónimamente, *axioma de pares no ordenados*]) (ZERMELO, 1908). Dados dos conjuntos s y t, existe un conjunto y, cuyos únicos elementos son s y t. En signos lógico-matemáticos,

$$\forall s \forall t \exists y \forall x (x \in y \leftrightarrow x = s \vee x = t).$$

Consecuencia de este axioma es que es admisible construir una sucesión infinita de conjuntos a partir del conjunto vacío; así, «después» del conjunto vacío, el primero sería tomar $s = \emptyset$ y $t = \emptyset$ y por el axioma de emparejamiento, aseguramos la existencia de un conjunto nuevo, a saber, el par no ordenado $\{\emptyset, \emptyset\}$ que abreviamos $\{\emptyset\}$ —de esta forma pudiésemos definir cualquier conjunto unitario (pero recordemos que por ahora el único conjunto del que tenemos asegurada su existencia es el vacío)—. De este modo, construimos los conjuntos «siguientes»: $\{\emptyset, \{\emptyset\}\}$, $\{\{\emptyset\}\}$, $\{\emptyset, \{\{\emptyset\}\}\}$, $\ldots$, si bien todos de dos elementos como mucho.

El *axioma de la unión* nos permitirá construir conjuntos con un número arbitrario de elementos.

§ 14.2.3 Axioma de la unión

Axioma de la unión (AU)

(CANTOR, 1899; ZERMELO, 1908). La unión de conjuntos es un conjunto. En signos lógico-matemáticos,

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists t (z \in t \wedge t \in x)).$$

O sea, para todo conjunto (de conjuntos) x, existe un conjunto y, formado por todos los elementos de los elementos de x, esto es, y es el conjunto unión de todos los elementos de x que notamos $\bigcup x$ o $\bigcup_{t \in x} t$ o $\bigcup\{t : t \in x\}$. Por ejemplo, si $x = \{\{a\}, \{b\}\}$, entonces la unión de los dos elementos de x es $\bigcup_{t \in x} t = \{a\} \cup \{b\} = \{a, b\}$.

Ahora sí que puede garantizarse la existencia de conjuntos con un número (natural) arbitrario de elementos, lo que le permite a ZERMELO construir los números naturales.

Definición 14.0.— Llamamos *sucesor* (o, sinónimamente, *siguiente*) de un conjunto x al conjunto $x \cup \{x\}$; designamos por Sx (o, sinónimamente, $x + 1$) a este nuevo conjunto.

Definición 14.1 (Números naturales (Zermelo)).—

$$0 \fallingdotseq \emptyset,$$
$$1 \fallingdotseq \{\emptyset\} \ (= \emptyset \cup \{\emptyset\}, \text{por AU}) (= S0),$$

$$2 \leftrightharpoons \{\emptyset, \{\emptyset\}\} \ (= \{\emptyset\} \cup \{\{\emptyset\}\}, \text{por AU})(= S1),$$
$$3 \leftrightharpoons \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \ (= \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\}, \text{por AU})(= S2),$$
$$\vdots$$

Observación 14.2.2.— Seguramente queda más claro la anterior definición utilizando los propios números naturales definidos:

$$0 \leftrightharpoons \emptyset,$$
$$1 \leftrightharpoons \{0\} \ (= 0 \cup \{0\}, \text{por AU})(= S0),$$
$$2 \leftrightharpoons \{0, 1\} \ (= 1 \cup \{1\}, \text{por AU})(= S1),$$
$$3 \leftrightharpoons \{0, 1, 2\} \ (= 2 \cup \{2\}, \text{por AU})(= S2),$$
$$\vdots$$
$$n + 1 \leftrightharpoons \{0, 1, \ldots, n\} \ (= n \cup \{n\}, \text{por AU})(= Sn)$$
$$\vdots$$

Observación 14.2.3.— Apreciamos claramente cómo los números naturales son conjuntos, concretamente, cada número natural es el conjunto de los números naturales construidos hasta ese momento.

§ 14.2.4 Axioma del conjunto potencia

Axioma del conjunto potencia (AP)

(o, sinónimamente, *axioma de las partes*) (ZERMELO, 1908). Para todo conjunto x existe el conjunto y de todos los subconjuntos de x. En signos lógico-matemáticos,

$$\forall x \exists y \forall z (z \in y \leftrightarrow z \subseteq x), \tag{14.1}$$

donde $z \subseteq x$ puede ser vista como una abreviatura de $\forall t(t \in z \to t \in x)$.

Observación 14.2.4.— Como sabemos, dicho conjunto se designa 2^x o $\mathcal{P}(x)$.

Aplicando este axioma es posible obtener la misma sucesión anterior $\emptyset, \mathcal{P}(\emptyset) = \{\emptyset\}, \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}, \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$, en la que, de hecho, la cardinalidad de cualquier término es mayor que la cardinalidad del inmediato anterior —por el teorema de CANTOR—. En definitiva, AP nos permite construir conjuntos de cardinalidad cada vez mayor.

Sin embargo, todas las cardinalidades que construimos con AP son finitas. Zermelo perseguía demostrar la hipótesis del continuo por lo que necesitaba asegurar que los conjuntos infinitos existieran. Para ello define los conceptos de *conjunto sucesor* (o *conjunto siguiente*) y *conjunto inductivo*.

Definición 14.2.— Llamamos *conjunto sucesor* (o, sinónimamente, *conjunto siguiente*) de/a un conjunto dado x al conjunto

$$x^+ = \bigcup\{x, \{x\}\} = x \cup \{x\}.$$

Definición 14.3.— Decimos que un conjunto x es un *conjunto inductivo* precisamente si contiene al conjunto vacío y es cerrado para la operación sucesor entre sus subconjuntos, esto es, si, y sólo si,

$$(\emptyset \in x) \wedge (\forall y(y \in x \to y^+ \in x)).$$

El *axioma del infinito* asegura la existencia de al menos un conjunto inductivo.

§ 14.2.5 Axioma del infinito

Axioma del infinito (AI)

(Zermelo, 1908). Existe un conjunto x, uno de cuyos elementos es el conjunto vacío, y x es tal que si y es elemento de x, entonces la unión de $y \cup \{y\}$ es elemento de x. En otras palabras, existe un conjunto x que es inductivo. En signos lógico-matemáticos,

$$\exists x(\emptyset \in x \wedge \forall y(y \in x \to y \cup \{y\} \in x)).$$

Como vemos, este axioma requiere la existencia del conjunto vacío, de ahí que en algunas presentaciones el sistema Z aparezca sin el axioma del conjunto vacío —al estimarlo presente implícitamente en el axioma del infinito—.

Este axioma permite a Zermelo demostrar que $\mathbb{N}$ es un conjunto; veamos cómo.

Teorema 14.4

ω es un conjunto.

Demostración.— Sean x un conjunto inductivo —existe precisamente por el axioma del infinito— y el conjunto de conjuntos $I(x) = \{y \in 2^x : y \text{ es inductivo}\}$. Como x es inductivo, $x \in I(x)$ y, por tanto, $I(x) \neq \emptyset$. Sea

$$\omega = \bigcap I(x),$$

donde

$$z \in \bigcap I(x) \text{ si, y sólo si, } (\forall y \in I(x))(z \in y). \tag{14.2}$$

■

En su global, los tres teoremas siguientes demuestran que, en el sentido de la inclusión de conjuntos, *ω es el único conjunto inductivo minimal*.

Teorema 14.5
ω es un conjunto inductivo.

Demostración.— Por una parte, $(\forall y \in I(x))(\emptyset \in y)$ [por ser inductivo todo conjunto y de $I(x)$], de donde $\emptyset \in \bigcap I(x)$ [por (14.2)]; por la otra, si $x \in \bigcap I(x)$, entonces $(\forall y \in I(x))(x \in y)$ [por (14.2)], de donde $(\forall y \in I(x))(x \cup \{x\} \in y)$ [ya que $(\forall y \in I(x))(y$ es inductivo$)$]. ∎

Teorema 14.6
Si y es un conjunto inductivo, entonces $\omega \subseteq y$.

Demostración.— Sea z un conjunto inductivo cualquiera, entonces $x \cap z \in I(x)$ [por definición de $I(x)$], de donde $\omega = \bigcap I(x) \subseteq x \cap z \subseteq z$ [por definición de intersección]. ∎

Teorema 14.7
Si y es inductivo e $y \subseteq \omega$, entonces $\omega = y$.

Demostración.— Como y es inductivo, entonces $\omega \subseteq y$ [por el teorema anterior]; también $y \subseteq \omega$ [por hipótesis]; de ambas, $\omega = y$ [por doble inclusión]. ∎

Precisamente, ZERMELO define el conjunto $\mathbb{N}$ de los números naturales como ω, de modo que

$$\begin{aligned}
0 &= \emptyset, \\
1 &= \emptyset^{+} = \{\emptyset, \{\emptyset\}\}, \\
2 &= 1^{+} = \{\emptyset, \{\emptyset\}\}^{+} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\
&\vdots
\end{aligned}$$

por lo que no sólo demuestra que $\mathbb{N}$ es un conjunto sino que es el menor conjunto inductivo.

El hecho de satisfacerse que $0 \subseteq 1 \subseteq 2 \subseteq 3 \subseteq \ldots$ permite a Zermelo definir una relación de orden total en $\mathbb{N}$.

Teorema 14.8
La relación $\leq$ definida $\forall m, n \in \mathbb{N}$ por

$$m \leq n \fallingdotseq m \subseteq n \tag{14.3}$$

es una relación de orden total en $\mathbb{N}$.

ZERMELO también define el concepto de *ordinal*.

Definición 14.4.— Decimos que un conjunto x es *ordinal* si, y sólo si,

I. x es un conjunto transitivo, esto es $\forall t \forall y((t \in y \wedge y \in x) \rightarrow t \in x)$,

II. $\in$ es un buen orden estricto, esto es,

 0. $\forall t(t \in x \rightarrow t \notin t)$, y
 1. $\forall t \forall y \forall z((t \in x \wedge y \in x \wedge z \in x \wedge t \in y \wedge y \in z) \rightarrow t \in z)$,
 2. $\forall y \subseteq x, y \neq \emptyset, \exists z \in y$ tal que $\forall t \in y(t \neq z \rightarrow z \in t)$ (z es un elemento minimal estricto en y respecto de $\in$).

Igualmente demuestra que los números naturales son ordinales y que el propio $\mathbb{N}$ también lo es —cuando consideramos $\mathbb{N}$ como ordinal lo designamos por ω, justamente el $\omega = \bigcap I(x)$ anterior—.

Teorema 14.9

Se satisface:

0. $\mathrm{ord}(0)$;
1. $(\forall x)(\mathrm{ord}(x) \rightarrow \mathrm{ord}(Sx))$;
2. $(\forall x)(x \in \omega \rightarrow \mathrm{ord}(x))$;
3. $\mathrm{ord}(\omega)$.

§ 14.3 Axiomática ZC (Z de Zermelo, C de *choice* [elección])

En relación con los órdenes buenos, Zermelo se propuso demostrar que todo conjunto puede ser bien ordenado —esto es, que para todo conjunto existe un orden total respecto del que todo subconjunto tiene un elemento minimal—. Para tal demostración necesitó de un nuevo axioma, el *axioma de elección*.

El sistema axiomático ZC está definido por los siguientes axiomas:

- axiomas del sistema axiomático Z;
- axioma de elección (AC).

§ 14.3.0 Axioma de elección

En el segundo Congreso Internacional de Matemáticas, celebrado en París en 1900, David Hilbert (1862-1943) propuso 23 problemas que según él deberían estar entre los que atrajesen a las mentes matemáticas del siglo XX. En el primero de ellos formuló dos cuestiones:

0. ¿Existe algún cardinal infinito entre $\aleph_0$ y $\mathfrak{c}$?

1. ¿Existe un buen orden para $\mathbb{R}$?

Axioma de elección (AC)

(LEVI, 1902 ; SCHMIDT, 1904 (citado en ZERMELO, 1904)). Para todo conjunto no vacío a, existe una aplicación $f : 2^a \setminus \{\emptyset\} \longrightarrow a$, tal que $\forall x \in a$, $f(x) \in x$.

Este axioma nos permite efectuar una «elección infinita» aunque no tengamos una propiedad que permita definir la función de elección y utilizar, en cambio, el axioma de reemplazamiento.

Dicho de otro modo, este axioma afirma:

> «Sea $M = \{A, B, C, \ldots\}$ una colección de conjuntos no vacíos, entonces existe un conjunto N que consta de un y sólo un elemento de A, uno de B, uno de C..., así sucesivamente a través de toda la colección de conjuntos M» (AC1).

Si M es finito, resulta intuitivo. El problema surge cuando M es infinito; en este caso, el axioma de elección equivale a admitir la posibilidad de efectuar una infinidad de elecciones arbitrarias. Pero la realidad es que no existe ningún método que permita escoger efectivamente uno a uno un elemento de cada conjunto de M.

El axioma de elección es equivalente a que el orden establecido entre los cardinales sea total.

En 1939, GÖDEL demuestra que tal axioma es consistente con los restantes axiomas de la teoría de conjuntos. Los matemáticos consideran que el axioma de elección no es lo suficientemente intuitivo como para ser aceptado entre los axiomas de la teoría de conjuntos; por otro lado, no es demostrable ni refutable a partir de dichos axiomas, pues en 1963, COHEN demuestra que el axioma de elección es independiente de los axiomas de la teoría de conjuntos, esto es, indecidible a partir de ellos—.

De este modo, surgen dos matemáticas, la que acepta el axioma de elección como uno de los de la teoría de conjuntos —matemáticas «zermelianas»— y la que no lo acepta —matemáticas no zermelianas—. Como el rechazo del axioma de elección implicaría el rechazo de importantes partes de las matemáticas «clásicas» y de la teoría de conjuntos, generalmente, en matemáticas se trabaja con él.

Volviendo a la sucesión $\mathfrak{C}$ de cardinales infinitos, y en relación con la primera cuestión del primer problema de HILBERT, pudiésemos preguntarnos si todo cardinal infinito es un elemento de la sucesión $\mathfrak{C}$. El siguiente teorema nos proporciona una respuesta.

Teorema 14.10
Si admitimos el axioma de elección, entonces todo número cardinal infinito, o bien coincide con un elemento de $\mathfrak{C}$, o bien puede ser inscrito entre dos elementos sucesivos de $\mathfrak{C}$.

Con respecto a la segunda cuestión del primer problema de HILBERT, su respuesta afirmativa —conocida como Teorema de ZERMELO— es equivalente al axioma de elección.

El siguiente teorema muestra diez formulaciones equivalentes del axioma de elección.

Teorema 14.11 (Diez formulaciones equivalentes del axioma de elección)

El axioma de elección es equivalente a cualquiera de las siguientes afirmaciones,

AC 0 Para todo conjunto no vacío A, existe una aplicación $f : 2^A \setminus \{\emptyset\} \longrightarrow A$, tal que $\forall x \subseteq A$, $f(X) \in X$ (esta aplicación se conoce como *función de elección*).

AC 1 (RUSSELL, 1906) Si $I \neq \emptyset$ y $\{A_i\}_{i \in I}$ es una familia de conjuntos no vacíos y mutuamente disjuntos, entonces existe un conjunto X que contiene exactamente un elemento de cada A_i.

AC 2 (ZERMELO, 1904) Puede darse un buen orden a todo conjunto (Teorema de ZERMELO). (La demostración es sólo existencial; realmente no se conoce aún ningún buen orden en $\mathbb{R}$).

AC 3 (ZORN, 1935) Todo conjunto inductivo posee un elemento maximal (Lema de ZORN).

AC 4 (RUSSELL, 1906) $I \neq \emptyset$ y $\{A_i\}_{i \in I}$ es una familia indexada de conjuntos no vacíos, entonces $\prod_{i \in I} A_i \neq \emptyset$.

AC 5 Si E es un conjunto no vacío, $G \subseteq E \times E$, $A = \text{dom}(G)$ y $B = \text{ran}(G)$, entonces existe una función $f : A \longrightarrow B$ tal que si Γ es su grafo, entonces $\Gamma \subseteq G$.

AC 6 (HAUSDORFF, 1909) Si A es un conjunto inductivo y $a \in A$, entonces existe un elemento m, maximal de A, tal que $a \leq m$.

AC 7 $f : A \longrightarrow B$ es una aplicación sobreyectiva si, y sólo si, existe una aplicación $g : B \longrightarrow A$, tal que $g \circ f = 1_B$.

AC 8 Sea A un conjunto cuyos elementos son conjuntos no vacíos y sea $B = \bigcup_{X \in A} X$, entonces, para toda función $g : A \longrightarrow A$, existe una función $g* : A \longrightarrow B$ tal que $\forall X \in A$, $g*(X) \in g(X)$.

AC 9 Si F es una familia de conjuntos no vacíos, disjuntos dos a dos, entonces existe una función f cuyo dominio es F y tal que para todo $A \in F$, $f(A) \in A$.

AC 10 Si B es un conjunto y $f : A \longrightarrow B$ una función, entonces existen $C \subseteq A$ y $g \subseteq f$ tales que $g : C \longrightarrow B$ es inyectiva y $\text{ran}(g) = \text{ran}(f)$.

§ 14.4 Axiomática ZF (Z de ZERMELO y F de FRAENKEL)

El sistema axiomático ZF está definido por los siguientes axiomas:

- axioma de extensionalidad (AE);
- axioma del conjunto vacío (AV);
- axioma de reemplazamiento (AR) (esquema de axiomas);
- axioma de la unión (AU);
- axioma del conjunto potencia (AP);

- axioma del infinito (AI);
- axioma de regularidad (ARe).

Como demostraremos, los axiomas de separación y emparejamiento, presentes en el sistema axiomático Z, son instancias del de reemplazamiento.

El axioma de regularidad es incorporado por ZERMELO en 1930.

Designamos por ZF^- el sistema axiomático de ZERMELO-FRAENKEL sin el axioma de regularidad.

§ 14.4.0 Esquema de axiomas de reemplazamiento

El axioma de reemplazamiento, al igual que los axiomas de ZERMELO de unión y conjunto potencia, es una instancia del axioma de comprensión, por lo que los conjuntos, cuya existencia se propugna, son únicos[5].

Este axioma viene a decir, informalmente, que cualquier propiedad («razonable») que pueda establecerse en el lenguaje formal de la teoría puede ser utilizada para definir un conjunto (el conjunto de los objetos que tienen esa propiedad)

Esquema de axiomas de reemplazamiento (AR)

(FRAENKEL, 1922; SKOLEM, 1923; versiones informales de CANTOR, 1899, y MIRIMANOFF, 1917).$\forall u, v, w(\psi(u, v) \wedge \psi(u, w) \rightarrow v = w) \rightarrow \forall z \exists y \forall v(v \in y \leftrightarrow (\exists u \in z)\psi(u, v))$, donde no hay ocurrencias libres de y ni de w en la fórmula $\psi(u, v)$, y $\psi(u, w)$ es la fórmula obtenida a partir de $\psi(u, v)$, sustituyendo w por v.

Este axioma es difícil de parafrasear. La hipótesis supone la existencia, para cada u, de como mucho, una v que verifique $\psi(u, v)$. Por ello, es admisible interpretar v como una función (parcial) de u, definida siempre que esta última exista. O sea, que tenemos una función parcial f, en u, tal que se satisface $\psi(u, f(u))$, siempre que $f(u)$ esté definida. El esquema axiomático de reemplazamiento afirma, entonces, la existencia de un conjunto y, formado exclusivamente por las imágenes por f de los elementos de z. Si $x_0, x_1, \ldots, x_k$, son variables libres de $\psi(u, v)$, distintas de u y v, es posible formalizarlas como parámetros, escribiendo $\psi(u, v)$, como $\psi(u, v; x_0, x_1, \ldots, x_k)$, y como, en este caso, el v que satisface $\psi(u, v; x_0, x_1, \ldots, x_k)$, depende de $u, x_0, x_1, \ldots, x_k$, entonces, AR afirma la existencia de un conjunto y, formado por aquéllos v que satisfagan que $(\exists u \in z)\psi(u, v; x_0, x_1, \ldots, x_k)$.

También es una instancia del axioma de comprensión.

Si definimos la teoría de conjuntos, en el marco de la lógica de primer orden, entonces, como $\exists x(x = x)$ es un teorema de ella, y nuestros únicos objetos son conjuntos, es aceptable suponer

[5] *Cfr. supra* observación 14.1.0 (pág. 756 de esta edición).

la existencia de al menos un conjunto. Entonces, no sería necesario el axioma del conjunto vacío, pues la existencia del conjunto vacío se deduciría del esquema axiomático de reemplazamiento: en efecto, bastaría tomar como $\psi(u,v)$ cualquier fórmula inválida, por ejemplo, $u \neq u$, de manera que el conjunto y, cuya existencia asegura AR, no tiene elementos. Sí es necesario el axioma del conjunto potencia, ya que según éste, y está definido mediante una propiedad y tal caso no está dado por el esquema axiomático de reemplazamiento, pues y no se define como el rango de una función.

El esquema axiomático de reemplazamiento permite construir nuevos axiomas. Por ejemplo, los siguientes teoremas demuestran que el axioma de separación y el de emparejamiento son instancias del de reemplazamiento.

Teorema 14.12
El axioma de separación es una instancia del axioma de reemplazamiento.

Demostración.— Si no hay ningún elemento que verifique $\phi(x)$, entonces, $y = \emptyset \subseteq x$. La demostración es consecuencia inmediata de AR, basta considerar $\psi(u,v) \equiv \phi(u) \wedge u = v$. ■

Teorema 14.13 (Corolario)
Si $\exists y \forall x(\phi(x) \to x \in y)$, entonces $\exists y \forall x(x \in y \leftrightarrow \phi(x))$.

Demostración.— Utilizando el axioma de separación. ■

Observación 14.4.0.— El axioma de separación no implica el esquema axiomático de reemplazamiento.

Observación 14.4.1.— Suelen llamarse versiones débiles de los axiomas de unión, conjunto potencia y reemplazamiento a los siguientes:

$$\mathrm{AU}_{\text{déb}} \equiv \forall x \exists y \forall z \forall u(z \in u \wedge u \in x \to z \in y);$$

$$\mathrm{AP}_{\text{déb}} \equiv \forall x \exists y \forall z(z \subseteq x \to z \in y);$$

$$\mathrm{AR}_{\text{déb}} \equiv \forall u,v,w(\psi(u,v) \wedge \psi(u,w) \to v = w) \to \forall z \exists y \forall u,v(u \in z \wedge \psi(u,v) \to v \in y).$$

Observación 14.4.2.— Debido al corolario 14.13 (pág. 767 de esta edición), podremos sustituir, según conveniencia, el conjunto de axiomas $\{\mathrm{AU}, \mathrm{AP}, \mathrm{AR}\}$, por $\{\mathrm{AU}_{\text{déb}}, \mathrm{AP}_{\text{déb}}, \mathrm{AR}_{\text{déb}}, \mathrm{AS}\}$. Por lo general, es más sencillo obtener un superconjunto de un conjunto deseado que el propio conjunto deseado.

Teorema 14.14
El axioma de emparejamiento es una instancia del axioma de reemplazamiento.

Demostración.— Consideremos AR, y sean $\psi(u,v) \equiv (u=\emptyset \wedge v=s) \vee (u=\{emptyset\} \wedge v=t)$ y $z=\{\emptyset,\{\emptyset\}\}$, entonces, el conjunto y, que existe por AR, tiene como únicos elementos s y t. ■

§ 14.4.1 Conjunto bien fundado

En ZC con el axioma de emparejamiento, los conjuntos pueden originarse a partir de tomar como entidades primitivas el conjunto vacío y un conjunto infinito e iterar los axiomas de separación, emparejamiento, unión, conjunto potencia y elección, lo cual permite que existan conjuntos *extraños* o *monstruosos* (*conjuntos no bien fundados*) como, por ejemplo, aquéllos que satisfacen que pertenecen a sí mismos. El axioma de regularidad no solventa tampoco este problema. Que puedan generarse estos monstruos es preocupante. Veamos a continuación los esfuerzos por evitarlos.

Para poder hablar con precisión de los conjuntos bien fundados necesitamos su definición, para lo cual, a su vez, necesitamos los conceptos previos de relación bien fundada, urelemento, conjunto transitivo y clausura transitiva de un conjunto.

Definición 14.5.— Decimos que una relación diádica R es una *relación bien fundada* en una clase X precisamente si todo subconjunto no vacío de X tiene un elemento minimal respecto de R, esto es, si, y sólo si, $(\forall S \subseteq X)\ (S \neq \emptyset \rightarrow (\exists m \in S)(\forall s \in S)\neg(sRm))$.

Una definición alternativa cuando se supone el axioma de elección es la siguiente.

Definición 14.6 (Relación bien fundada (suponiendo AC)).— Suponiendo el axioma de elección, equivalentemente, decimos que una relación diádica R es una *relación bien fundada* en X precisamente si X no contiene ninguna cadena descendiente infinita para R, esto es, si, y sólo si, no existe ninguna secuencia infinita $x_0, x_1, \ldots, x_n, x_{n+1}, \ldots$ de elementos de X tal que $(\forall n \in \mathbb{N})(x_{n+1} R x_n)$.

Definición 14.7.— Decimos que x es un *conjunto transitivo* si, y sólo si, se satisface alguna de las condiciones equivalentes siguientes:

0. si $t \in s \wedge s \in x$, entonces $t \in x$;
1. si $s \in x \wedge s$ no es un urelemento, entonces $s \subseteq x$.

entendiendo por *urelemento* una entidad (abstracta o concreta) que no es un conjunto si bien sí puede ser un elemento de un conjunto. (Una clase es transitiva precisamente si todo elemento de la clase es un subconjunto de la clase).

Definición 14.8.— La *clausura transitiva de un conjunto* x es el conjunto transitivo más pequeño (en el sentido de la inclusión de conjuntos) que incluye a x.

Definición 14.9.— Decimos de un conjunto x que es un *conjunto bien fundado* si, y sólo si, la relación de pertenencia $\in$ es una relación bien fundada en la clausura transitiva de x.

§ 14.4.2 Axioma de regularidad

Este axioma nace con el propósito de asegurar que todos los conjuntos sean bien fundados. Sobre ello, Fraenkel hizo una propuesta —e independientemente Skolem (1923)— que fue revisada por John von Neumann en 1925, proponiendo el axioma de regularidad, si bien no lo incluyó en sus sistema axiomático. Fue Zermelo en 1930 quien primero lo incluye. Actualmente suele incluirse en el sistema axiomático ZF.

Axioma de regularidad (ARe)

(o también, *axioma de fundamentación*) (Skolem, 1923, Neumann, 1925) (adoptado por Zermelo en 1930). $\exists x \phi(x) \to \exists x(\phi(x) \land (\forall y \in x)\neg\phi(y))$, donde y está ligada en $\phi(y)$.

Como hemos dicho, ARe prohíbe conjuntos no bien fundados, por ejemplo, conjuntos autorreferentes, esto es, afirmaciones como $x \in x$ o $x = \{x\}$ ya no están permitidas.

Teorema 14.15 (Formulación equivalente de ARe)
Este axioma puede formularse, equivalentemente: $\forall x(x \neq \emptyset \to (\exists y \in x)(x \cap y = \emptyset))$.

Ejemplo 398

La clase de todos los conjuntos, *la clase universal* —el universo de los conjuntos—, V, es una clase propia.

Resolución.— Lo demostramos por reducción al absurdo. Supongamos que V es un conjunto, entonces:

0. por un lado, por el *axioma del par*[6], $\{V\}$ también es un conjunto, de donde, por el *axioma de regularidad*[7], en $\{V\}$ debe existir un elemento disjunto con V y como el único elemento de $\{V\}$ es V, se tiene que $V \cap \{V\} = \emptyset$;

1. por otro, como por su propia definición V incluye a todos los conjuntos y por hipótesis de RAA es un conjunto, se tiene que $V \in V$ y como también ocurre que $V \in \{V\}$, por definición de intersección de conjuntos, $V \in V \cap \{V\}$, de donde $V \cap \{V\} \neq \emptyset$;

he aquí, pues, una contradicción, $V \cap \{V\}$ es a la vez vacía y no vacía, por lo que por RAA, V no es un conjunto. ■

[6] *Vid. infra* § 14.2.2 (pág. 759 de esta edición).
[7] *Vid. infra* § 14.4.2 (pág. 769 de esta edición]).

Ejemplo 399

Demostremos que la clase $R = \{x : x \notin x\}$ es precisamente la clase universal $V = \{x : x = x\}$ y, por lo tanto, que $R = \{x : x \notin x\}$ es una clase propia —de hecho, vimos cómo considerarla un conjunto lleva a contradicción (paradoja de Russell)—.

Resolución.— Demostremos que $\forall x, x \notin x$, en otras palabras, que todo conjunto x está en R. En efecto, sea x un conjunto, por un lado, por el *axioma del par*[8], $\{x\}$ es un conjunto, por otro, por el *axioma de regularidad*[9], existe un elemento y de $\{x\}$ tal que $y \cap \{x\} = \emptyset$, pero como el único elemento de $\{x\}$ es x, eso significa que $x \cap \{x\} = \emptyset$, de donde, por las definiciones de intersección y de conjunto vacío, x no puede ser un elemento de x.

Hemos visto que todo conjunto x se caracteriza por satisfacer $x \notin x$, por lo que la clase universal puede también definirse como $V = \{x : x \notin x\}$, en otras palabras, $V = R$ y, por lo tanto, R es una clase propia, debido a que V lo es[10]. ■

§ 14.5 Axiomáticas ZFC y ZFC⁻

El sistema axiomático ZFC está definido por los siguientes axiomas:

- axiomas del sistema axiomático ZF;
- axioma de elección (AC).

Designamos por ZFC⁻ el sistema axiomático ZFC sin el axioma de regularidad.

§ 14.6 Otras axiomáticas

A lo largo de los años, se han creado variados sistemas axiomáticos alternativos —*cfr. v. gr.* https://en.wikipedia.org/wiki/Alternative_set_theory y https://plato.stanford.edu/entries/settheory-alternative/—, por ejemplo, el sistema axiomático de Neumann-Bernays-Gödel (NBG), de cuyos axiomas también es independiente el axioma de regularidad. Con NBG, aún no siendo éste lógicamente equivalente a ZFC —pues su fuerza expresiva es mayor (en ZFC sólo se trabaja con conjuntos, en NBG con conjuntos y clases)—, se obtienen los mismos resultados sobre conjuntos que pueden obtenerse en ZFC (técnicamente se dice que NBG *extiende conservativamente* a ZFC).

[8] *Vid. infra* § 14.2.2 (pág. 759 de esta edición).
[9] *Vid. infra* § 14.4.2 (pág. 769 de esta edición).
[10] *Vid. supra* ejemplo 398 (pág. 769 de esta edición).

§ 14.7 Hipótesis del continuo

Retomando el primer problema de HILBERT, en su apartado uno, y ya sea admitiendo o no el axioma de elección, lo que no se puede, en un principio, es descartar que entre $\aleph_0$ y $\mathfrak{c}$, existan cardinales diferentes de ambos, ni que, en general, tampoco existan otros cardinales entre cualesquiera dos términos sucesivos de la sucesión de cardinales infinitos $\mathfrak{c}$.

¿Qué ordinal α es tal que $\aleph_\alpha = 2^{\aleph_0}$? CANTOR planteó esta cuestión, que conocemos como *problema del continuo*. CANTOR buscaba encontrar un conjunto cuyo cardinal estuviese entre $\aleph_0$ y $\mathfrak{c}$.

CANTOR conjetura que no existen cardinales entre $\aleph_0$ y $2^{\aleph_0} = \mathfrak{c}$, es decir, conjetura que $\aleph_1$ sería $\mathfrak{c}$, afirmación que actualmente se conoce como *hipótesis del continuo* (HC): $2^{\aleph_0} = \aleph_1$. En 1883, implícitamente, CANTOR también conjetura que $2^{\aleph_1} = \aleph_2$.

La conjetura más general, de que cualquiera que sea el número cardinal infinito $\mathfrak{k}$, no existen otros números cardinales entre $\mathfrak{k}$ y $2^{\mathfrak{k}}$, es decir, que los números cardinales son única y exclusivamente los recogidos en la sucesión $\mathfrak{C}$, fue formulada por vez primera por HAUSDORFF (1908), se conoce como *hipótesis general del continuo* (HGC) y afirma, como hemos comentado, que $2^{\aleph_i} = \aleph_{i+1}, \forall i \in \mathbb{N}$.

En 1938, GÖDEL, demuestra que HGC es consistente con ZFC, o sea, que HC no puede ser refutada a partir de ZF ni de ZFC. En 1963, COHEN demuestra que incluso HC *no es decidible* a partir de ellos, o sea, que a partir de los axiomas usuales de la teoría de conjuntos, ya sea con el axioma de elección o sin él —ZFC o ZF, respectivamente—, es imposible demostrar la veracidad (COHEN) o la falsedad (GÖDEL), ni de HC ni de HGC. Estos resultados de GÖDEL y COHEN, se obtienen bajo la hipótesis de la consistencia de ZF.

¿Qué lugar ocupa $\mathfrak{c}$ en la escala de alephs?

Resulta que también es consistente suponer cualquiera de las igualdades $2^{\aleph_0} = \aleph_2$, $2^{\aleph_0} = \aleph_3$, etc., es decir, no sabemos nada sobre la magnitud de $2^{\aleph_0}$ comparada con la de $\aleph_i$. Por tanto, es consistente con ZFC, suponer, por ejemplo, que $2^{\aleph_0}$ es un cardinal intermedio entre $\aleph_1$ y $2^{\aleph_1}$ ($\aleph_1 < 2^{\aleph_0} < 2^{\aleph_1}$).

Los resultados de GÖDEL y COHEN también demuestran, siendo ZF consistente, la independencia del axioma de elección respecto de ZF, es decir, que no es decidible a partir de ellos. Pudiese argumentarse la posibilidad de admitir HC, o incluso HGC, o sus negaciones, como axioma, y extender ZF. Sin embargo, esta elevación a la categoría de axioma de una afirmación, debe ser corroborada con la experiencia y, como mínimo, debe ser suficientemente intuitiva —lo intuitivo que era el postulado de las paralelas de EUCLIDES, y sin embargo...(pero ésta es otra historia)—.

Resulta más intuitivo el axioma de elección que HC; por ello, que no presente demasiada objeción el admitir AC como axioma. De hecho, la matemática actual se desarrolla en el sistema axiomático ZFC admitiendo HGC, que designaremos por ZFC+HGC.

§ 14.8 Relación con la teoría de la computación

Sea cual sea el programa, desde el punto de vista de su codificación en una máquina clásica (no cuántica), es una mera hilera de bits, por lo que la acción del programa corresponde a calcular una función $f : \mathbb{N} \longrightarrow \mathbb{N}$. Pudiésemos pensar, entonces, que a toda función $f : \mathbb{N} \longrightarrow \mathbb{N}$, le correspondería un programa, que pudiese ser implementado en alguna ocasión. Sea $F = \{f \text{ tal que } f : \mathbb{N} \longrightarrow \mathbb{N}\}$, resulta que $F \approx 2^{\mathbb{N}}$. Es decir, existe una cantidad no numerable de tales funciones.

En la actualidad, hay un número finito de lenguajes de programación, éstos se basan en un alfabeto finito y los programas tienen una cantidad finita de letras, por lo que es posible listar todos los posibles programas, primero, todos los de longitud una letra, luego, los de longitud dos, a continuación, los de longitud tres, etc. Claramente, la cantidad de programas es numerable.

Una cantidad no numerable de funciones $f : \mathbb{N} \longrightarrow \mathbb{N}$, y una cantidad numerable de programas. Admitiendo que cualquier programa calcula una única función, entonces existen funciones no calculables por ningún programa —funciones no computables—.

Incluso contando con los programas que calculan un número finito de funciones o, incluso, programas que calculan un número infinito numerable de funciones (un ejemplo de ellos son los *programas universales*), como la unión numerable de conjuntos numerables es numerable[11], la cantidad total de funciones calculables es numerable.

¿Se conocen alguna de estas funciones no computables? ¿Se conocen todas?, esto es, ¿se conoce alguna caracterización de ellas? ¿Es posible computarlas, utilizando otro lenguaje de programación, o una máquina de mayor potencia? Son preguntas cuyas respuestas corresponden a la teoría de la computación.

La actualidad está dominada por alfabetos finitos y programas implementados con un número finito de líneas de código. ¿Es posible modificar esta situación? Por ejemplo, ¿pudiésemos permitir,

- un alfabeto infinito numerable, para lo cual bastaría tener un símbolo e indexarlo con un conjunto infinito numerable, por ejemplo, $\{a_i : i \in \mathbb{N}\}$, o
- un número infinito de líneas de código?

Surgen también cuestiones acerca de su de procesamiento y ejecución —¿reducible siempre a secuencial?, ¿cómo escribir infinitas líneas de código? ¿cómo computarlas?—. El programa $(\forall \mathrm{i})(\mathrm{PRINT\ i})$ tiene infinitas líneas de programa, representables —compactables— en una única. En otras palabras, es un programa infinito para el que existe un programa finitamente representable, equivalente —misma solución—.

[11] *Cfr. supra* teorema 13.16 (pág. 732 de esta edición).

§ 14.9 Números algebraicos y trascendentes

Definición 14.10.— Un número real que es raíz de algún polinomio con coeficientes enteros, se llama algebraico[12].

Ejemplo 400

Demostremos que $\sqrt{2}$ y el número áureo ϕ, esto es, $(1+\sqrt{5})/2$, son algebraicos.

Resolución.— Por un lado, $\sqrt{2}$ satisface la ecuación $x^2 - 2 = 0$, es decir, es raíz del polinomio con coeficientes enteros $x^2 - 2$; por otro, el número áureo es raíz del polinomio con coeficientes enteros $x^2 - x - 1$. ■

Números metálicos, la matemática y el diseño

El número áureo es un caso particular de *número metálico*. Éstos son las raíces positivas de polinomios cuadráticos de la forma

$$x^2 - px - q,$$

con p y q enteros positivos.

Por ejemplo:

- si $p = q = 1$, el *número de oro*, la raíz positiva $(1+\sqrt{5})/2 = 1{,}6180339887\ldots$;
- si $p = 2$ y $q = 1$, el *número de plata*, la raíz positiva $1+\sqrt{2} = 2{,}4142135623\ldots$;
- si $p = 3$ y $q = 1$, el *número de bronce*, la raíz positiva $(3+\sqrt{13})/2 = 3{,}3027756377\ldots$;
- si $p = 4$ y $q = 1$, el *número de cobre*, la raíz positiva $2+\sqrt{5} = 4{,}2360679774\ldots$;
- si $p = 5$ y $q = 1$, el *número de níquel*, la raíz positiva $(5+\sqrt{29})/2 = 5{,}1925824035\ldots$;
- y, en general, si $p = n$ y $q = 1$, el *número metálico enésimo*, la raíz positiva $(n+\sqrt{n^2+4})/2$.

Resulta que, dada la sucesión de números de Fibonacci, esto es, el problema de valores iniciales* $f(0) = 0$, $f(1) = 1$, $f(n+2) = f(n+1) + f(n)$, el número de oro es límite de $f(n+2)/f(n+1)$ cuando n tiende a infinito.

Algo similar sucede con el resto de números metálicos: si definimos la familia de *sucesiones generalizadas de* Fibonacci *secundarias* por $g(0) = 0$, $g(1) = 1$, $g(n+2) =$

[12] Puede que encontremos en la literatura otras definiciones de números algebraicos, por ejemplo, aquéllos que son raíces reales de polinomios con coeficientes racionales, o bien, aquéllos que son raíces reales de polinomios con coeficientes números algebraicos (observemos el carácter recursivo de esta última definición). Las tres definiciones que aparecen en esta página son equivalentes.

$p \cdot g(n+1) + q \cdot g(n)$, con p y q enteros positivos, resulta que cada número metálico es límite cuando n tiende a infinito de $g(n+2)/g(n+1)$ para alguna sucesión concreta g. Por ejemplo, el número de oro para $p = q = 1$ y el número de plata para $p = 2$ y $q = 1$.[†]

[*] *Cfr. infra* definición 20.13 (pág. 1302 de esta edición).
[†] *Vid. v. gr.* https://itc.scix.net/pdfs/4856.content.pdf (véase aquí también su relación con la matemática y el diseño).

Otros ejemplos de números algebraicos son i y $\cos\left(\frac{\pi}{n}\right)$ ($n \in \mathbb{Z}^+$).

Teorema 14.16
Los números racionales son los números algebraicos solución de un polinomio de grado uno con coeficientes enteros.

Demostración.— En efecto, el número racional p/q es solución del polinomio de grado uno con coeficientes racionales $qx - p$. ■

Al conjunto de todos los números reales algebraicos lo designamos por $\mathbb{A}$.

Teorema 14.17
$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{A}$.

Por otro lado, es usual notar $X[x]$ al conjunto de todos los polinomios, en la variable x, con coeficientes elementos de X; así, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ y $\mathbb{R}[x]$ designan los conjuntos de todos los polinomios, en la variable x, con coeficientes enteros, racionales y reales, respectivamente.

Definición 14.11.— Un *número trascendente* es aquél que no es raíz de un polinomio con coeficientes enteros, por ejemplo, e y π.

Los primeros ejemplos de números trascendentes los proporciona Liouville, en 1844. Posteriormente, Hermite demuestra, en 1873, que e es trascendente, y Lindemann demuestra, en 1882, que π también lo es[13].

Al conjunto de todos los números reales trascendentes, lo designamos por $\mathbb{T}$.

Con respecto a la cardinalidad de $\mathbb{A}$ y $\mathbb{T}$, Cantor demuestra, en 1874 que $|\mathbb{A}| = \aleph_0$ y que $|\mathbb{T}| = \mathfrak{c}$.

[13] Mahler proporcionó un ejemplo de número trascendente que, seguramente, nos sorprenda: 0,123456789101112131415 . . . El teorema de Gelfond-Schneider proporciona un método fácil de generación de números trascendentes: si a es un número real algebraico distinto de 0 y de 1, y b es un número algebraico irracional, entonces ab es trascendente. Así, por ejemplo, $2^{\sqrt{2}}$ es trascendente. A pesar de ello, son muchas las cuestiones sobre números trascendentes que permanecen abiertas; un ejemplo: aunque sepamos que e y π son trascendentes, no sabemos si $e + \pi$ o $e\pi$ son trascendentes (no obstante, sabemos que uno de ellos ha de serlo, investiguemos el polinomio $x2 - (e + \pi)x + e\pi$) (citaremos otro ejemplo en teoría de la computabilidad).

§ 14.10 Número ordinal

§ 14.10.0 Semejanza entre conjuntos ordenados

Definición 14.12.— Sean dos conjuntos totalmente ordenados $(X; \preccurlyeq)$ y $(Y; \preccurlyeq')$ y una aplicación $f : X \longrightarrow Y$. Entonces:

0. f es *isótona* si, y sólo si, $(\forall x, y)(x \preccurlyeq y \to f(x) \preccurlyeq' f(y))$;

1. f es una *semejanza* si, y sólo si, f es biyectiva y f y f^{-1} son isótonas.

Definición 14.13.— Decimos que $(X; \preccurlyeq)$ e $(Y; \preccurlyeq')$ son semejantes si, y sólo si, existe alguna (aplicación de) *semejanza* entre ellos. Este hecho lo expresamos por $(X, \preccurlyeq) \cong (Y, \preccurlyeq')$.

Teorema 14.18
$\cong$ es una relación diádica de equivalencia en cualquier colección de conjuntos totalmente ordenados.

Teorema 14.19
Dados dos conjuntos totalmente ordenados, o bien son semejantes, o bien, uno de ellos es semejante a una sección inicial del otro.

Teorema 14.20
Un conjunto bien ordenado no es semejante a ninguna sección inicial suya.

§ 14.10.1 Tipo de orden y número ordinal

Definición 14.14 (Tipo de orden).— (Cantor, 1895). Llamamos *tipo de orden* (o, sinónimamente, *tipo ordinal*) a cualquier clase de equivalencia de la relación $\cong$. De este modo, el tipo de orden de $(X; \preccurlyeq)$ es $\overline{(X; \preccurlyeq)} = \{(Y; \preccurlyeq') : (X, \preccurlyeq) \cong (Y, \preccurlyeq')\}$. En otras palabras, $\overline{(X; \preccurlyeq)} = \overline{(Y; \preccurlyeq')}$ (esto es, $(X; \preccurlyeq)$ e $(Y; \preccurlyeq')$ tienen el mismo tipo de orden) si, y sólo si, $(X; \preccurlyeq)$ e $(Y; \preccurlyeq')$ son semejantes.

Definición 14.15.— Llamamos *número ordinal* (o simplemente, *ordinal*) al tipo de orden de un conjunto bien ordenado.

§ 14.10.2 Números naturales

Teorema 14.21
Existe un menor ordinal transfinito, que es, precisamente, $\overline{(\mathbb{N};\leq)}$, con $\leq$ el orden habitual en $\mathbb{N}$. Designamos dicho ordinal por ω.

Demostración.— En efecto, sea $\overline{(X;\preccurlyeq)}$ otro ordinal tal que $\overline{(X;\preccurlyeq)} < \omega$, entonces del teorema 14.19 (pág. 775 de esta edición) se sigue que, o bien $(X;\preccurlyeq) \cong (\mathbb{N};\leq)$, con lo que se trataría del mismo ordinal, o bien $(X;\preccurlyeq)$ es semejante a una sección inicial de $(\mathbb{N};\leq)$, que es un subconjunto finito de números naturales, y por tanto, X es finito, siendo entonces $\overline{(X;\preccurlyeq)}$ un ordinal finito. ■

§ 14.10.3 Ordinales y cardinales

Definición 14.16.— Llamamos *cardinal de un número ordinal* al cardinal de cualquier conjunto bien ordenado cuyo tipo de orden sea el número ordinal.

No es difícil darnos cuenta de que para cualquier conjunto finito X de cardinal n, existen $n!$ buenas ordenaciones de X (tantas como permutaciones distintas de los elementos de X). Pero estos $n!$ buenos órdenes, definen el mismo ordinal[14], es decir, si X e Y son conjuntos finitos, entonces $|X| = |Y|$ si, y sólo si, $\overline{(X;\preccurlyeq)} = \overline{(Y;\preccurlyeq')}$. Por esto, los ordinales finitos pueden identificarse con los cardinales finitos $0, 1, 2, \ldots$

La situación para los ordinales transfinitos no es la misma. En general, aseguramos lo que establece el siguiente teorema.

Teorema 14.22
Si $(X,\preccurlyeq) \cong (Y,\preccurlyeq')$, entonces $|X| = |Y|$.

¿Qué sucede con el recíproco?

Sí es verdad que si dos conjuntos finitos de igual cardinal son ambos totalmente ordenados, entonces están bien ordenados y son semejantes —lo hemos comentado justo antes del teorema, en este caso, el recuento de los elementos es independiente de cómo se ordenen; en otras palabras, todos los conjuntos bien ordenados que provengan de un mismo conjunto finito o de otro conjunto equipotente con éste, son semejantes—. De aquí que el cardinal finito se identifique con un ordinal.

El caso transfinito es distinto. En esta situación, el recíproco del teorema no es cierto. Dos conjuntos bien ordenados pueden tener el mismo cardinal sin ser semejantes —las diferentes ordenaciones de los elementos no son equivalentes, pudiendo generar diferentes ordinales—. Veamos un ejemplo de esto último que servirá, a su vez, de contraejemplo del recíproco del teorema.

[14] *Cfr. supra* teorema 14.20 (pág. 775 de esta edición).

Ejemplo 401

Encontremos un contraejemplo para el recíproco del teorema 14.22 (pág. 776 de esta edición).

Resolución.— Consideremos en $\mathbb{N}$, el orden bueno $\leq'$, definido por $1 \leq' 2 \leq' 3 \leq' \ldots \leq' 0$, es decir, hemos añadido un máximo, el 0, al conjunto bien ordenado $(\mathbb{Z}^+; \leq)$. Se satisface que $|\mathbb{Z}^+| = |\mathbb{N}|$ y que $\overline{(\mathbb{Z}^+; \leq)} = \overline{(\mathbb{N}; \leq)}$. Sin embargo, $\overline{(\mathbb{N}; \leq)} = \omega$ y $\overline{(\mathbb{N}; \leq')} = \omega + 1$; en efecto, $\overline{(\mathbb{N}; \leq)} = \omega < \omega + 1 = \overline{(\mathbb{Z}^+; \leq)} + \overline{(\{0\}; \leq)} = \overline{(\mathbb{N}; \leq')}$. Éste visto es un contraejemplo para el recíproco del teorema 14.22 (pág. 776 de esta edición) —basta tomar $(X; \preccurlyeq) = (\mathbb{N}; \leq)$ e $(Y; \preccurlyeq') = (\mathbb{N}; \leq')$—. ■

§ 14.10.4 Sucesión transfinita de números ordinales

Operaciones entre ordinales

Es posible definir la suma de ordinales, el producto de ordinales y la exponenciación ordinal. Sin entrar en los detalles formales, aquí sólo diremos algo sobre la suma.

Definición 14.17.— Dados los ordinales α y β con $(X; \preccurlyeq)$ e $(Y; \preccurlyeq')$ tales que $\overline{(X; \preccurlyeq)} = \alpha$, $\overline{(Y; \preccurlyeq')} = \beta$ y $X \cap Y = \emptyset$, definimos $\alpha + \beta$ como $\overline{(X \cup Y; \preccurlyeq'')}$, estando $\preccurlyeq''$ definida $\forall x, y \in X \cup Y$ por $x \preccurlyeq'' y$ si, y sólo si, $(x, y) \in X \times Y$ o $x \preccurlyeq y$ o $x \preccurlyeq' y$.

Teorema 14.23

La suma no es conmutativa.

Demostración.— Por ejemplo, $1 + \omega = \omega \neq \omega + 1$. Del primero, un ejemplo es la reunión ordenada de $(\{0\}; \leq)$ y $(\mathbb{N}; \leq)$, esto es, el conjunto bien ordenado $(0 \leq) 0 \leq 1 \leq 2 \leq \ldots$; del segundo, la reunión ordenada de $(\mathbb{N}; \leq)$ y $(\{0\}; \leq)$, es decir, $1 \leq 2 \leq 3 \leq \ldots \leq 0$. ■

Ejemplo 402

¿Cuáles son los números ordinales de los siguientes conjuntos bien ordenados?

- $3 \leq 4 \leq 5 \leq \ldots \leq 0 \leq 1 \leq 2$;
- $0 \leq 2 \leq 4 \leq \ldots \leq 1 \leq 3 \leq 5 \leq \ldots$;
- $0 \leq 3 \leq 6 \leq \ldots \leq 1 \leq 4 \leq 7 \leq \ldots \leq 2 \leq 5 \leq 8 \leq \ldots$;
- $0 \leq 4 \leq 8 \leq \ldots \leq 1 \leq 5 \leq 9 \leq \ldots \leq 2 \leq 6 \leq 10 \leq \ldots \leq 3 \leq 7 \leq 11 \leq \ldots$

Resolución.— Son $\omega + 3$, 2ω, 3ω y 4ω, respectivamente. ■

Génesis de los ordinales

Teorema 14.24
Si al conjunto bien ordenado $(X; \preccurlyeq)$ cuyo tipo de orden es el número ordinal α le añadimos un nuevo elemento, digamos ζ, tal que $\forall x \in X, x \preccurlyeq \zeta$ y que ζ sea máximo del nuevo conjunto, entonces el tipo de orden del conjunto bien ordenado que obtenemos, $\overline{(X \cup \{\zeta\}; \preccurlyeq)}$, representa al ordinal siguiente a α, que designamos $\alpha + 1$.

Así, los ordinales finitos,

$$\begin{aligned}
&0, \\
1 &= \overline{(\{0\} \cup \{1\}; 0 \leq 1)} \quad (= 0 + 1), \\
2 &= \overline{(\{0, 1\} \cup \{2\}; 0 \leq 1 \leq 2)} \quad (= 1 + 1), \\
3 &= \overline{(\{0, 1, 2\} \cup \{3\}; 0 \leq 1 \leq 2 \leq 3)} \quad (= 2 + 1), \\
&\vdots \\
n + 1 &= \overline{(\{0, 1, 2, \ldots, n\} \cup \{n + 1\}; 0 \leq 1 \leq 2 \leq \ldots \leq n \leq n + 1)} \quad (= n + 1), \\
&\vdots
\end{aligned}$$

y los ordinales transfinitos,

$$\begin{aligned}
&\omega, \\
\omega + 1 &= \overline{(\omega \cup \{\omega\}; 0 \leq 1 \leq 2 \leq \ldots \leq \omega)}, \\
\omega + 2 &= \overline{(\omega \cup \{\omega, \omega + 1\}; 0 \leq 1 \leq 2 \leq \ldots \leq \omega \leq \omega + 1)}, \\
&\vdots \\
\omega + n + 1 &= \overline{(\omega \cup \{\omega, \omega + 1, \ldots, \omega + n\}; 0 \leq 1 \leq 2 \leq \ldots \leq \omega \leq \omega + 1 \leq \ldots \leq \omega + n)}, \\
&\vdots \\
2\omega & \quad (\text{esto es, } \omega + \omega), \\
2\omega + 1 &= \overline{(\omega \cup \{\omega, \omega + 1, \ldots, \omega + \omega\}; 0 \leq 1 \leq 2 \leq \ldots \leq \omega \leq \omega + 1 \leq \ldots \leq \omega + \omega)}, \\
&\vdots \\
3\omega & \quad (\text{esto es, } 2\omega + \omega), \\
3\omega + 1 &= \overline{(\omega \cup \{\omega, \omega + 1, \ldots, 3\omega\}; 0 \leq 1 \leq 2 \leq \ldots \leq \omega \leq \omega + 1 \leq \ldots \leq 3\omega)}, \\
&\vdots \\
\omega^2 & \quad (\text{esto es, } \omega \cdot \omega), \\
&\vdots
\end{aligned}$$

De la sucesión transfinita emerge de inmediato una *clasificación dicotómica de los números ordinales*:

- por una parte, aquéllos que tienen un predecesor directo en la sucesión transfinita, esto es, 1, 2, 3, ..., $\omega + 1$, $\omega + 2$, $\omega + 3$, ...;
- por otra, aquéllos que no tienen un predecesor directo en dicha sucesión, esto es, 0, ω, 2ω, 3ω, ..., ω^2, ω^3, ...

Estos últimos no son construibles por el procedimiento visto; son supremos de los conjuntos respectivos de ordinales menores que ellos, pero no son máximos. Decimos que son ordinales límite.

Definición 14.18.— Un *ordinal límite* es cualquier ordinal distinto de cero, que no sea sucesor de ningún otro ordinal.

Estudiamos otra clasificación de interés en § 14.10.6 (pág. 780 de esta edición).

§ 14.10.5 Buen orden entre ordinales

Definición 14.19.— La relación $\leq$ entre ordinales definida, dados dos números ordinales α y β, por $\beta \leq \alpha$ si, y sólo si, existen dos conjuntos bien ordenados $(X; \preccurlyeq)$ e $(Y; \preccurlyeq')$ tales que $\alpha = \overline{(X; \preccurlyeq)}$, $\beta = \overline{(Y; \preccurlyeq')}$ e $(Y; \preccurlyeq')$ es una sección inicial de $(X; \preccurlyeq)$, es una relación de buen orden entre ordinales.

Definición 14.20.— Dado un ordinal α, designamos por $\mathbb{O}_{<\alpha}$ al conjunto de los ordinales menores que α, esto es, al conjunto $\{\beta : \beta \leq \alpha \text{ y } \beta \neq \alpha\}$. Este conjunto $\mathbb{O}_{<\alpha}$ es una *sección inicial abierta de números ordinales*.

Observación 14.10.0.— De manera natural, definimos una biyección entre números ordinales y secciones iniciales abiertas de números ordinales: $\alpha \mapsto \mathbb{O}_{<\alpha}$ y $\mathbb{O}_{<\alpha} \mapsto \alpha$.

Teorema 14.25
$\overline{\mathbb{O}_{<\alpha}} = \alpha$.

Ejemplo 403

Comprobemos cómo $\overline{\mathbb{O}_{<0}} = 0$, $\overline{\mathbb{O}_{<n}} = n$, $\overline{\mathbb{O}_{<\omega}} = \omega$ y $\overline{\mathbb{O}_{<\omega+k}} = \omega+k$, para $k \in \mathbb{Z}^+$.

Resolución.— $\overline{\mathbb{O}_{<0}} = 0$ porque no existen números ordinales anteriores a 0; $\overline{\mathbb{O}_{<n}} = n$ ya que a n le preceden los números ordinales 0, 1, ..., $n - 1$, que son n; $\overline{\mathbb{O}_{<\omega}} = \omega$ porque a ω le anteceden los ω ordinales 0, 1, 2, ..., y $\overline{\mathbb{O}_{<\omega+k}} = \omega + k$ porque a $\omega + k$ le preceden los ordinales, 0, 1, 2, ..., ω, $\omega + 1$, ..., $\omega + (k - 1)$. ■

Actividad 14.0

¿Pueden ser semejantes dos secciones iniciales de ordinales distintas?

Teorema 14.26 (Antinomia/Paradoja de Burali-Forti)
(O también, *paradoja del mayor número ordinal*). (Burali-Forti, 1897).
No existe ningún conjunto que incluya a todos los ordinales como elementos.

Demostración.— Sea la clase bien ordenada $(\mathbb{O}; \leq)$ de todos los números ordinales y consideremos su número ordinal $\overline{(\mathbb{O}; \leq)}$, pues bien, resulta que $\overline{(\mathbb{O}; \leq)} \notin \mathbb{O}$ porque de lo contrario, también sucedería que $\overline{(\mathbb{O}; \leq)}+1 \in \mathbb{O}$, pero $\overline{(\mathbb{O}; \leq)} < \overline{(\mathbb{O}; \leq)}+1$, por lo que $\overline{(\mathbb{O}; \leq)}$ no sería el número ordinal de todos los ordinales. ■

Observación 14.10.1.— De este modo, todos los números ordinales son, por definición, elementos de $\mathbb{O}$, pero por otro lado, no todos los números ordinales son elementos de $\mathbb{O}$, pues $\overline{(\mathbb{O}; \leq)}$ no lo es. He aquí lo paradójico.

Observación 14.10.2.— Dicen que Cantor, en 1895, descubrió la paradoja de Burali-Forti y también la conocida como *paradoja de* Cantor. Éste demostró que el cardinal del conjunto potencia de un conjunto es mayor que el cardinal de dicho conjunto y, sin embargo, si el conjunto es el conjunto de todos los conjuntos, todos sus subconjuntos son, a la vez, elementos suyos, por lo que es imposible que existan más subconjuntos que elementos.

§ 14.10.6 Clase ordinal

Definición 14.21.— Si $\mathfrak{a}$ es un cardinal, llamamos *clase ordinal* y designamos por $\overline{\mathfrak{a}}$ a la colección de todos los ordinales de cardinal $\mathfrak{a}$.

Teorema 14.27
Si $\mathfrak{a}$ es finito, entonces $|\overline{\mathfrak{a}}| = 1$.

Teorema 14.28
Si $\mathfrak{a}$ es transfinito, entonces $\mathfrak{a} < |\overline{\mathfrak{a}}|$.

Teorema 14.29
$\aleph_0 < |\overline{\aleph_0}|$.

Demostración.— El cardinal de la primera clase de ordinales transfinitos, cuyos elementos son ω, $\omega+1$, $\omega+2$, ..., es mayor o igual que $\aleph_0$. Demostremos que debe ser mayor que $\aleph_0$. Para ello, razonemos por reducción al absurdo: si fuese $\aleph_0$, éste sería el cardinal del conjunto formado por los

ordinales finitos y por los de $\overline{\aleph_0}$, pero esto no es posible, pues este conjunto es la sección inicial de ordinales $\mathbb{O}_{<\alpha}$ para un cierto ordinal α y si $|\mathbb{O}_{<\alpha}|$ fuese $\aleph_0$, como el tipo ordinal de $\mathbb{O}_{<\alpha}$ es α, entonces $|\alpha| = \aleph_0$, por lo que α estaría en la primera clase, lo que no es posible, ya que $\alpha \notin \mathbb{O}_{<\alpha}$. En definitiva, $\aleph_0 < |\overline{\aleph_0}|$. ■

Designemos $|\overline{\aleph_0}|$ por $\aleph_1$. Este $\aleph_1$ es también el cardinal de ω_1, el menor ordinal transfinito no perteneciente a $\overline{\aleph_0}$, de modo que ω_1 y todos los ordinales de cardinal $\aleph_1$ constituyen la segunda clase de ordinales transfinitos, cuyo cardinal, que designamos por $\aleph_2$, es mayor que $\aleph_1$ y es el cardinal de ω_2, el menor ordinal transfinito no perteneciente a $\overline{\aleph_0}$ ni a $\overline{\aleph_1}$. Y así sucesivamente, formándose una sucesión transfinita estrictamente creciente de números ordinales $\omega, \omega_1, \omega_2, \ldots, \omega_\omega, \omega_{\omega+1}, \ldots$ (en paralelo a la sucesión de los álef, $\aleph_0, \aleph_1, \aleph_2, \ldots, \aleph_\omega, \aleph_{\omega+1}, \ldots$) que llamamos *ordinales iniciales*.

Observación 14.10.3.— Es posible trazar biyecciones entre los álef, los ordinales iniciales y todos los números ordinales:

$$\begin{array}{ccccccc} \aleph_0 & \aleph_1 & \aleph_2 & \ldots & \aleph_\omega & \aleph_{\omega+1} & \ldots \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \\ \omega & \omega_1 & \omega_2 & \ldots & \omega_\omega & \omega_{\omega+1} & \ldots \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \\ 0 & 1 & 2 & \ldots & \omega & \omega+1 & \ldots \end{array}$$

Teorema 14.30
El cardinal de un conjunto infinito bien ordenado es un álef.

Demostración.— Su número ordinal es de una de las clases de ordinales transfinitos y, por definición de clase ordinal, todos los ordinales en ella tienen el mismo cardinal, un álef según lo anterior. ■

§ 14.10.7 Lema de Zorn y axioma de Zermelo

Definición 14.22.— De un conjunto ordenado tal que todo subconjunto suyo totalmente ordenado posea supremo, decimos que es un *conjunto inductivo* (o, sinónimamente, un *conjunto inductivamente ordenado*).

Teorema 14.31 (Lema de Zorn)
(Kuratowski, 1922; Zorn, 1935).
Todo conjunto inductivo tiene al menos un elemento maximal.

Teorema 14.32 (Teorema del buen orden; Zermelo; ZFC$^-$)
(O sinónimamente, *axioma de* Zermelo, 1904).
Todo conjunto admite un buen orden.

Teorema 14.33
Todo número cardinal transfinito es un álef.

Demostración.— Admitiendo el axioma de elección, la hipótesis general del continuo permite definir una biyección entre la sucesión de ordinales iniciales y la sucesión de cardinales (sucesión de potencias de dos):

$$\begin{array}{cccccccc} \aleph_0 & \aleph_1 & \aleph_2 & \dots & \aleph_\omega & \aleph_{\omega+1} & \dots \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \updownarrow & \\ \aleph_0 & 2^{\aleph_0} & 2^{2^{\aleph_0}} & \dots & \Omega_0 & 2^{\Omega_0} & \dots \end{array}$$

■

Teorema 14.34 (De numeración)
Todo conjunto es equipotente a algún ordinal.

Teorema 14.35
En ZF$^-$ son equivalentes el axioma de elección, el lema de Zorn y el axioma de Zermelo.

§ 14.11 Propuesta de más actividades

Actividad 14.1

En el teorema 14.11 (pág. 765 de esta edición), demostremos las equivalencias de la AC5 a la AC10.

Actividad 14.2

El conjunto y que aparece en el axioma del conjunto potencia (*cfr. supra* ejemplo 14.2.4 [pág. 760 de esta edición]) está definido mediante una propiedad, pero, entonces, ¿no sería este axioma una consecuencia del axioma de reemplazamiento?

Actividad 14.3

Demostremos que utilizando las siguientes fórmulas $\phi(x)$, obtenemos refutaciones del axioma de comprensión de Frege:

0. $\neg\exists z(x \in z \land z \in x)$;
1. $\neg\exists z_0, z_1, \dots, z_n(x \in z_0 \land z_0 \in z_1 \land \dots \land z_{n-1} \in z_n \land z_n \in x)$.

Actividad 14.4

¿Es admisible reformular el axioma de regularidad así: $\forall x \exists y(x = \emptyset \wedge (y \in x \wedge \forall z(z \in x \to \neg z \in y)))$?

§ 14.12 Bibliografía

- Primeros pasos:

  [182] Francesc Rossell i Pujós. *El infinito. ¿Es un viaje o un destino?* Grandes ideas de las matemáticas. EMSE EDAPP y Prisanoticias Colecciones, Barcelona, Cataluña (ES-CT), España, 2019.

  [183] Julián Garrido Garrido. *Verdad matemática: introducción a los fundamentos de la matemática*. Ciencia abierta. Nivola, Madrid, Comunidad de Madrid (ES-M), España, 2003.

  [188] Carlos Ivorra Castillo. *Lógica y teoría de conjuntos*. Autoedición, Valencia, Comunidad Valenciana [ES-VC], España, 2022. https://www.uv.es/ivorra/Libros/Logica.pdf (accedido el 26.1.2024). ©gratisOA.

- Posibles segundos:

  [148] Karel Hrbacek y Thomas J. Jech. *Introduction to set theory*. Monographs and textbooks in pure and applied mathematics. Marcel Dekker, Nueva York, Nueva York (US-NY), Estados Unidos de América, 3.ª ed., 1999.

  [184] Azriel Levy. *Basic Set Theory*. Perspectives in Mathematical Logic Series. Springer-Verlag, Berlin - Heidelberg - New York, 1979.

  [185] Keith James Devlin. *Fundamentals of Contemporary Set Theory*. Springer - Verlag, New York - Heidelberg - Berlin, 1979.

  [186] Gaisi Takeuti y Wilson Miles Zaring. *Introduction to Axiomatic Set Theory*. Springer - Verlag, New York - Heidelberg - Berlin, 1971.

- Posibles terceros:

  [142] José Antonio Alonso Jiménez, Joaquín Borrego Díaz, Mario de Jesús Pérez Jiménez y José Luis Ruiz Reina. *Curso Práctico de Teoría de Conjuntos*. La Ñ, Sevilla, Andalucía (ES-AN), España, 1998.

Capítulo 15

Lógica de la construcción del sistema numérico

Hay dos razones por las que es estúpido definir los números naturales como $\{1, 2, 3, 4, \ldots\}$ en lugar de $\{0, 1, 2, 3, \ldots\}$. Primera, ya tenemos un nombre perfecto para el conjunto $\{1, 2, 3, 4, \ldots\}$, a saber, el conjunto de números enteros positivos. Segunda, al excluir el cero de los números naturales se convierte en «antinatural» y este hecho de que para muchas personas el número «cero» aún sea un ciudadano de segunda es un obstáculo estándar en el pensamiento matemático.

(Edsger Wybe DIJKSTRA, 1930–2002,
A notational alternative for quantification, pág. 4 [nota], 30.04.1980,
https://www.cs.utexas.edu/users/EWD/ewd07xx/EWD737.PDF).°

«Como es el pan será la sopa». Este refrán español transmite la profunda conexión entre la materia prima, los cimientos, los fundamentos, y la calidad de lo que se construye con ella. Responde en este punto a nuestro querer conocer la procedencia de la consistencia del sistema numérico.

§ 15.0 Números naturales

En este subcapítulo nos acercamos a la estructura del semianillo conmutativo, unitario, íntegro, bien ordenado y arquimediano $(\mathbb{N}; +, \cdot; \leq)$ de los números naturales.

° Notemos que en algunos textos en los que se denomina a $\{1, 2, 3, 4, \ldots\}$ el conjunto de números naturales, se denomina el conjunto de números completos (*whole numbers*) a $\{0, 1, 2, 3, \ldots\}$.

§ 15.0.0 Axiomas de Peano

Giuseppe PEANO proporcionó en 1889 una definición axiomática del conjunto de números naturales, mediante cinco axiomas, utilizando tres conceptos primitivos, «número« (número natural), «cero» (un primer número) y la función (relación diádica) s, «ser sucesor de» (o «siguiente a»).[1]

Axiomas de Peano

I. *Axioma de existencia.* $0 \in \mathbb{N}$, esto es, *cero es un número*;

-. *Axiomas de la relación de igualdad* (en el marco de la lógica de primer orden con identidad[2] no son necesarios):

- -.0 $(\forall n \in \mathbb{N})(n = n)$ (todo número es igual a sí mismo, en otras palabras, la relación de igualdad es reflexiva);
- -.1 $(\forall m, n \in \mathbb{N})(m = n \rightarrow n = m)$ (la relación de igualdad es simétrica);
- -.2 $(\forall l, m, n \in \mathbb{N})(l = m \wedge m = n \rightarrow l = n)$ (la relación de igualdad es transitiva);
- -.3 $(\forall m, n \in \mathbb{N})(m = n \wedge n \in \mathbb{N} \rightarrow m \in \mathbb{N})$ ($\mathbb{N}$ es cerrado para la relación de igualdad);

II. *Axioma de estabilidad.* $(\forall n \in \mathbb{N})(s(n) \in \mathbb{N})$ (*si n es un número, entonces el sucesor de n también es un número*)($\mathbb{N}$ es cerrado para s);

III. *Axioma del mínimo.* $(\forall n \in \mathbb{N})(s(n) \neq 0)$ (*cero no es el sucesor de ningún número*);

IV. *Axioma de extensibilidad.* $(\forall m, n \in \mathbb{N})(s(m) = s(n) \rightarrow m = n)$ (*si los sucesores de dos números son iguales, entonces los números mismos son iguales*) (s es inyectiva);

V. *Axioma de inducción.* $(\forall C \subseteq \mathbb{N})(0 \in C \wedge \forall n \in C, s(n) \in C \rightarrow C = \mathbb{N})$ (*si un conjunto de números C contiene al cero y también al sucesor de cualquier número que pertenezca a C, entonces todo número pertenece a C*).

---

[1] Ésta, la del cuadro, es, en lenguaje lógico-matemático moderno, la primera versión de su axiomática que aparece en *Arithmetices principia* (1889) (en realidad, en esta primera versión, PEANO eligió comenzar en 1, si bien nosotros, con su versión final de 1908 y con ZERMELO, empezamos en 0.); en *Formulaire de mathématique* (1897-1899), ya desaparecieron los cuatro axiomas de la relación de igualdad (al él estimarlos pertenecientes más a la lógica); en *Formulario mathematico, volumen V* (1908) aparecen en *latino sine flexione* seis axiomas: *.0* $N_0 \varepsilon$ *Cls. .1* $0 \varepsilon N_0$. *.2* $a \varepsilon N_0 . \supset .a + \varepsilon N_0$. *.3* $s \varepsilon$ *Cls* $. 0 \varepsilon s : a \varepsilon s . \supset_a . a + \varepsilon s : \supset .N_0 \supset s$ *Induct. .4* $a, b \varepsilon . N_0 . a+ = b+ . \supset .a = b$. *.5* $a \varepsilon N_0 . \supset .a + - = 0$. Lege: *.0* N_0 *es classe, vel numero es nomen commune. .1 Zero es numero. .2 Si a es numero, tunc suo successivo es numero. .3* N_0 *es classe minimo, que satisfac ad conditione .0.1.2 id es, si s es classe, que contine 0 et si a pertine ad classe s, seque pro omni valore che a, que et a+pertine ad s; tunc omni numero es s. Ce propositione es dicto principio de inductione, et nos indica illo per abbreviatione Induct. Omni conditione determina uno classe, ergo nos pote lege principio de inductione sub forma: Si s es conditione, satisfacto ab numero 0, et si omni vice que illo es vero pro numero a, et es vero pro suo successivo, tunc conditione s es vero pro omni numero. .4 Duo numero, que habe successivo æquale, es æquale inter se. .5 0 non seque nullo numero.*

[2] *Vid. supra* § 5.6.0 (pág. 423 de esta edición).

Ejemplo 404

Demostremos que $0 \neq 1$.

Resolución.— Se tiene que 0 es un número [axioma I]; el sucesor de 0, que llamamos 1, también es un número [axioma II]; 0 es distinto del sucesor de cualquier número [axioma III] y 1 es un sucesor, por lo que 0 no puede ser 1. ■

Ejemplo 405

Demostremos que $0 \neq 2$.

Resolución.— Como $2 = s(1)$ y 0 es distinto del sucesor de cualquier número [axioma III], 0 no puede ser 2. ■

Observación 15.0.0.— De una manera análoga, demostraríamos que $0 \neq n$, para todo $n > 0$.

Ejemplo 406

Demostremos que todo número es distinto de sus anteriores.

Resolución.— Como $0 \neq 1$, $s(0) \neq s(1)$ [axioma IV] (por contrapositiva), esto es, $1 \neq 2$; como $1 \neq 2$, $s(1) \neq s(2)$ [axioma IV] (por contrapositiva), esto es, $2 \neq 3$; como $0 \neq 2$, $s(0) \neq s(2)$ [axioma IV] (por contrapositiva), esto es, $1 \neq 3$; por lo tanto, 1, 2 y 3 son distintos entre sí y también distintos de 0 (observación inmediatamente anterior); y así sucesivamente; ahora, siendo C el conjunto de los números que son distintos a todos sus anteriores, vemos que $C = \mathbb{N}$ [axioma V]. ■

Observación 15.0.1.— En este último ejemplo hemos hecho una *demostración por inducción*. Aprenderemos más sobre ellas en § 16 (pág. 804 de esta edición).

§ 15.0.1 Aritmética

En base a los axiomas de Peano es posible definir la *suma* (y el *producto*) de números naturales, como una función o relación que asocia a cada pareja de números naturales, (m, n), otro número natural.[3]

[3] Aunque el ser humano ha sumado y multiplicado números desde tiempos ancestrales, no es hasta que George Cantor crea la teoría de conjuntos y se asienta la definición de cardinal[4] , cuando puede definirse formalmente la suma de números naturales a partir de definir el número natural n como el cardinal de un conjunto finito de n elementos, de manera que $m + n$ se define como el cardinal de la unión de dos conjuntos finitos disjuntos de cardinales m y n.

[4] *Vid. supra* § 13.1.1 (pág. 719 de esta edición).

Definición 15.0 (Suma de números naturales).— $\forall m, n \in \mathbb{N}$, definimos el *número natural suma de* m *y* n, y lo designamos por $m + n$, en la forma:

$$m + 0 = m,$$
$$m + \text{suc}(n) = \text{suc}(m + n).$$

Definición 15.1 (Producto de números naturales).— $\forall m, n \in \mathbb{N}$, definimos el *número natural producto de* m *y* n, y lo designamos por $m \cdot n$, en la forma:

$$m \cdot 0 = 0,$$
$$m \cdot \text{suc}(n) = (m \cdot n) + m.$$

Observación 15.0.2.— Estas definiciones son implícitas, de tipo inductivas, de forma, que para conocer la suma de dos números naturales hay que proceder del siguiente modo, para así, conocer la suma $m + (n + 1)$, en función de la suma $(m + n)$, (análogamente para el producto):

$$\begin{aligned} m + 1 &= m + \text{suc}(0) = \text{suc}(m + 0) = \text{suc}(m) \\ m + 2 &= m + \text{suc}(1) = \text{suc}(m + 1) \\ m + 3 &= m + \text{suc}(2) = \text{suc}(m + 2) \\ &\vdots \\ m + (n + 1) &= m + \text{suc}(n) = \text{suc}(m + n) \end{aligned}$$

Observemos que a partir de la definición de suma, obtenemos que $m + 1 = \text{suc}(m)$, $m + 2 = \text{suc}(m + 1)$, . . ., para lo que sólo debemos asegurar que $1 = \text{suc}(0)$.

A partir de los axiomas y de las anteriores definiciones inductivas, es posible demostrar algunas propiedades básicas de $+$ y $\cdot$ en $\mathbb{N}$.

Teorema 15.0 (Propiedades de $+$ en $\mathbb{N}$)

En $(\mathbb{N}; +)$ se satisface:

0. $(\forall l, m, n \in \mathbb{N})((l + m) + n = l + (m + n))$; (asociativa de $+$)
1. $(\forall m, n \in \mathbb{N})(m + n = n + m)$; (conmutativa de $+$)
2. $(\forall n \in \mathbb{N})(0 + n = n + 0 = n)$; (elemento neutro de $+$)
3. $(\forall l, m, n \in \mathbb{N})(l + n = m + n \to l = m)$. (cancelación para $+$)

Teorema 15.1 (Propiedades de $\cdot$ en $\mathbb{N}$)
En $(\mathbb{N};\cdot)$ se satisface:

0. $(\forall l, m, n \in \mathbb{N})((l \cdot m) \cdot n = l \cdot (m \cdot n))$; (asociativa de $\cdot$)
1. $(\forall m, n \in \mathbb{N})(m \cdot n = n \cdot m)$; (conmutativa de $\cdot$)
2. $(\forall n \in \mathbb{N})(1 \cdot n = n \cdot 1 = n)$; (elemento neutro de $\cdot$)
3. $(\forall l, m, n \in \mathbb{N})(n \neq 0 \to (l \cdot n = m \cdot n \to l = m))$. (cancelación para $\cdot$)

Teorema 15.2 (Propiedades de $+$ y $\cdot$ en $\mathbb{N}$)
En $(\mathbb{N};+,\cdot)$ se satisface:

0. $(\forall l, m, n \in \mathbb{N})(l \cdot (m + n) = l \cdot m + l \cdot n)$; (distribución de $\cdot$ en $+$)
1. $(\forall l, m, n \in \mathbb{N})((l + m) \cdot n = l \cdot n + m \cdot n)$. (distribución de $\cdot$ en $+$)

§ 15.0.2 Axiomática de la aritmética elemental

Rayano con cuando estudiamos diversos sistemas axiomáticos para la teoría de conjuntos[5], pudiésemos definir la aritmética en $\mathbb{N}$ como un sistema basado, en última instancia, en la lógica de primer orden.

Recordemos que la extensión aritmética[6] $\mathcal{L}_1^+$ del lenguaje $\mathcal{L}_1$ de la lógica de primer orden, resulta de añadir a éste, además del signo de igualdad, $=$ (constante predicativa), los signos correspondientes a las funciones adición y multiplicación, $+$ y $\cdot$ (constantes funtoriales), y los nombres propios de los números $0, 1, 2, \ldots$ —para éstos, una vez que ya sabemos construirlos, utilizaremos el nombre propio del cero, 0, y el funtor monádico suc denotativo de la operación «sucesor de»—; éstos serán los signos primitivos, las constantes aritméticas.

El conjunto de los números naturales $\mathbb{N}$ es el dominio de referencia, el conjunto universal, por lo que pudiésemos considerar a los dos primeros axiomas de Peano como meras reglas gramaticales, esto es, como reglas de formación de fórmulas bien formadas del sistema.

Por lo tanto, la aritmética elemental en $\mathbb{N}$ es, y sólo es, ésta así definida:

Axiomas de igualdad:

$$(\forall x, y)(x = y \to \mathrm{suc}(x) = \mathrm{suc}(y));$$
$$(\forall x, y, z)(x = y \to (x = z \to y = z));$$

Axiomas de Peano:

$$(\forall x, y)(\mathrm{suc}(x) = \mathrm{suc}(y) \to x = y);$$
$$(\forall x)(\neg\, \mathrm{suc}(x) = 0);$$

[5] *Vid. supra* § 14 (p. 752).
[6] *Vid. supra* § 5.6.2 (pág. 429 de esta edición).

$$P0 \land (\forall x)(Px \to P\,\mathrm{suc}(x)) \to \forall y P y;^{(*)}$$

Axiomas de la suma:

$$(\forall x)(x + 0 = x);$$
$$(\forall x, y)(x + \mathrm{suc}(y) = \mathrm{suc}(x + y));$$

Axiomas del producto:

$$(\forall x)(x \cdot 0 = 0);$$
$$(\forall x, y)(x \cdot \mathrm{suc}(y) = x \cdot y + x);$$

Regla de inducción:$^{(*)}$

$$\begin{array}{ll} & P0 \\ & (\forall x)(Px \to P\,\mathrm{suc}(x)) \\ \hline \therefore & \forall y P y \end{array}$$

No obstante, si bien hemos afirmado que esta axiomatización se basa, en última instancia, en la lógica de primer orden, debiésemos precisar, por una parte, que al utilizar la igualdad, ésta pertenece a la lógica de primer orden con identidad[7], y por otra, que en la formalización de la inducción, pudiésemos considerar las letras predicativas como parámetros susceptibles de ser interpretados como «cualquier predicado», en cuyo caso, este sistema se asienta en la lógica de primer orden (con identidad), o como variables, admitiendo cuantificaciones de dichos predicados, perteneciendo entonces esta formalización a la lógica de segundo orden[8] (con identidad).

Observación 15.0.3.— Con la interpretación paramétrica de las letras predicativas, la teoría de la aritmética elemental es un ejemplo de *teoría de primer orden* —una teoría que puede ser fundamentada, formalizada y axiomatizada a partir sólo de la lógica de primer orden—. En estas notas aparecerá, como otro ejemplo explícito, la *teoría de grupos*[9], si bien son muchas más[10]. A modo de ejemplo, en otras disciplinas, un par de ellas: en biología, la *teoría de la genética clásica*, axiomatizada por Joseph Henry Woodger[11] (53 axiomas), y en economía, la *teoría de la utilidad esperada*[12], axiomatizada por John von Neumann y Oskar Morgenstern[13] (4 axiomas[14]).

[7] *Vid. supra* § 5.6.0 (pág. 423 de esta edición).
[8] *Vid. supra* pág. 372.
[9] *Vid. infra* observación 17.5.1 (p. 850).
[10] *Vid. v. gr.* https://human.libretexts.org/Bookshelves/Philosophy/Logic_and_Reasoning/Sets_Logic_Computation_(Zach)/02%3A_II-_First-order_Logic/2.02%3A_Theories_and_Their_Models/2.2.03%3A_Examples_of_First-Order_Theories y https://en.wikipedia.org/wiki/List_of_first-order_theories.
[11] *Vid.* Joseph Henry Woodger, 1952, *Biology and language: an introduction to the methodology of the biological sciences including medicine*, Cambridge: Cambridge University Press.
[12] *Vid. v. gr.* https://plato.stanford.edu/archives/win2018/entries/bounded-rationality.
[13] *Vid.* John von Neumann y Oskar Morgenstern, 1944, *Theory of Games and Economic Behavior*, Princeton, NJ: Princeton University Press.
[14] *Vid. v. gr.* https://en.wikipedia.org/wiki/Expected_utility_hypothesis#The_von_Neumann%E2%80%93Morgenstern_axioms.

§ 15.0.3 Orden

Definición 15.2 (Relaciones diádicas $\leq$ y $<$ en $(\mathbb{N};+)$).— Definimos en $(\mathbb{N};+)$ las relaciones diádicas $\leq$ y $<$:

0. $(\forall m,n\in\mathbb{N})\,(m\leq n\leftrightarrow(\exists k\in\mathbb{N})(m+k=n))$;
1. $(\forall m,n\in\mathbb{N})\,(m<n\leftrightarrow(\exists k\in\mathbb{N}^{+})(m+k=n))$.

Teorema 15.3 (Interdefiniciones de $\leq$ y $<$)

Se satisface:

0. $(\forall m,n\in\mathbb{N})\,(m\leq n\leftrightarrow m<n\vee m=n)$;
1. $(\forall m,n\in\mathbb{N})\,(m<n\leftrightarrow m\leq n\wedge m\neq n)$.

Teorema 15.4

La relación diádica $\leq$ es un orden total en $(\mathbb{N};+)$, esto es, se caracteriza por ser reflexiva, antisimétrica, transitiva y conexa:

I. $(\forall n\in\mathbb{N})(n\leq n)$; (reflexiva)
II. $(\forall m,n\in\mathbb{N})(m\leq n\wedge n\leq m\rightarrow m=n)$; (antisimétrica)
III. $(\forall l,m,n\in\mathbb{N})(l\leq m\wedge m\leq n\rightarrow l\leq n)$; (transitiva)
IV. $(\forall m,n\in\mathbb{N})(m\leq n\vee n\leq m)$; (conexa)

Teorema 15.5

La relación diádica $<$ es un orden parcial estricto en $(\mathbb{N};+)$, esto es, se caracteriza por ser irreflexiva y transitiva:

I. $(\forall n\in\mathbb{N})(n\not<n)$; (irreflexiva)
II. $(\forall l,m,n\in\mathbb{N})(l<m\wedge m<n\rightarrow l<n)$. (transitiva)

Teorema 15.6

En $(\mathbb{N};+,\cdot)$, la relación $\leq$ satisface las propiedades de monotonía y cancelación:

0. $(\forall k,m,n\in\mathbb{N})(m\leq n\leftrightarrow m+k\leq n+k)$; (monotonía para $+$)
1. $(\forall k,m,n\in\mathbb{N})(k>0\rightarrow(m\leq n\leftrightarrow m\cdot k\leq n\cdot k))$; (monotonía para $\cdot$)
2. $(\forall k,m,n\in\mathbb{N})(m+k=n+k\rightarrow m=n)$; (cancelación para $+$)
3. $(\forall k,m,n\in\mathbb{N})(k\neq 0\rightarrow(m\cdot k=n\cdot k\rightarrow m=n))$. (cancelación para $\cdot$)

Teorema 15.7

La relación $\leq$ es un *buen orden* en $(\mathbb{N};+)$, esto es, todo subconjunto no vacío de $\mathbb{N}$ tiene primer elemento con respecto a la relación $\leq$.

Teorema 15.8
Sean $m, n \in \mathbb{N}$. Que la *ecuación* $m + x = n$ tenga solución en $(\mathbb{N}; +)$ es equivalente a que $m \leq n$.

Definición 15.3.— Dados $m, n \in \mathbb{N}$, llamamos *diferencia* de n y m y la designamos por $n - m$, a la solución de la *ecuación* $m + x = n$, cuando ésta exista en $(\mathbb{N}; +)$.

Teorema 15.9
Se satisface:
0. $(\forall m, n \in \mathbb{N})(m \leq n \leftrightarrow n - m \in \mathbb{N})$;
1. $(\forall m, n \in \mathbb{N})(m < n \leftrightarrow n - m \in \mathbb{N}^+)$.

Teorema 15.10
$(\mathbb{N}; +, \cdot; \leq)$ satisface la *propiedad arquimediana*[15], esto es, $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N}^+)(\exists k \in \mathbb{N}^+)(m < k \cdot n)$.

Teorema 15.11 (Algunas estructuras algebraicas presentes en $(\mathbb{N}; +, \cdot; \leq)$)
(*Cfr. infra* § 17 [pág. 834 de esta edición]).
0. $(\mathbb{N}; +; \leq)$ es un monoide conmutativo, unitario y bien ordenado;
1. $(\mathbb{N}; \cdot; \leq)$ es un monoide conmutativo, unitario y bien ordenado;
2. $(\mathbb{N}; +, \cdot; \leq)$ es un semianillo conmutativo, unitario, íntegro, bien ordenado y arquimediano.

§ 15.1 Números enteros

En este subcapítulo nos acercamos a la estructura del anillo conmutativo, unitario, íntegro, totalmente ordenado y arquimediano $(\mathbb{Z}; +, \cdot; \leq)$ de los números enteros.

§ 15.1.0 Un porqué

No toda ecuación tiene solución en $(\mathbb{N}; +)$, por ejemplo,

$$x + 1 = 0.$$

Se puede remediar esta falta introduciendo los números no positivos, $\mathbb{N}_0^- = \{\ldots, -3, -2, -1, 0\}$, formándose el conjunto $\mathbb{Z} = \mathbb{N} \cup \mathbb{N}_0^-$, de números enteros.

[15] *Cfr. infra* observación 17.12.5 (pág. 917 de esta edición).

Decimos que $\mathbb{N}_0^-$ es el *simetrizado* de $\mathbb{N}$. Además, es posible demostrar que $\mathbb{N}_0^-$ es único. De este modo, todo número —futuro número entero— tiene simétrico respecto de $+$, número que conocemos como su *opuesto*.

Por $\mathbb{N}^-$ designamos el conjunto de los números negativos, esto es, $\mathbb{N}^- = \mathbb{N}_0^- \setminus \{0\}$.

§ 15.1.1 Construcción de $\mathbb{Z}$

Consideramos en $\mathbb{N} \times \mathbb{N}$ la relación

$$(\forall \langle k, l\rangle, \langle m, n\rangle \in \mathbb{N} \times \mathbb{N})(\langle k, l\rangle E \langle m, n\rangle \leftrightarrow k + n = l + m).$$

Esta relación es de equivalencia. Por un lado, expresa todas las posibles diferencias que puede haber entre dos números naturales, y, por otro, clasifica estas diferencias. Las clases de equivalencia, $[\langle 0, n\rangle]$, $[\langle 0, 0\rangle]$ y $[\langle n, 0\rangle]$, corresponden a las diferencias $-n$, 0 y n, respectivamente; y por ello, precisamente, suelen notarse así. En otras palabras, el conjunto $\mathbb{Z}$ de números enteros no es más que el conjunto cociente $\mathbb{N} \times \mathbb{N}/_E$, y un número entero, n, por tanto, no es más que:

$$n = \begin{cases} [\langle 0, n\rangle] & \text{si} \quad n < 0 \\ [\langle 0, 0\rangle] & \text{si} \quad n = 0 \\ [\langle n, 0\rangle] & \text{si} \quad n > 0 \end{cases}$$

Actividad 15.0

Relacionemos esta construcción con lo estudiado en el ejemplo 336 (pág. 634).

Observación 15.1.0.— Por $\mathbb{Z}^*$, $\mathbb{Z}^+$, $\mathbb{Z}_0^+$, $\mathbb{Z}^-$ y $\mathbb{Z}_0^-$, notamos, respectivamente, los enteros sin el cero, los enteros positivos, éstos más el cero (los naturales), los enteros negativos y éstos más el cero (simetrizado de los naturales). Siendo $n \in \mathbb{N}^+$, es habitual notar por $\mathbb{N}_n$ o $[n]$ al conjunto $\{0, 1, \ldots, n-1\}$ y por $\mathbb{N}_n^+$ o $[n]^+$ al conjunto $\{1, \ldots, n-1\}$ (la notación $\mathbb{Z}_n$, a veces empleada, puede ser confusa).

§ 15.1.2 Aritmética

Definición 15.4 (Signo de un número entero).— Signo (sgn) es la función definida por:

$$\begin{aligned} \operatorname{sgn} : \mathbb{Z} &\longrightarrow \{-1, 0, 1\} \\ n &\longmapsto \operatorname{sgn}(n) = \begin{cases} -1 & \text{si} \quad n \in \mathbb{Z}^-, \\ 0 & \text{si} \quad n = 0, \\ 1 & \text{si} \quad n \in \mathbb{Z}^+. \end{cases} \end{aligned}$$

Definición 15.5 (Suma y producto de números enteros).— Definimos las operaciones diádicas suma y producto en $\mathbb{Z}$ en función de las de $\mathbb{N}$, a través de la definición de dichas operaciones en $\mathbb{N} \times \mathbb{N}$:

$\forall \langle k, l\rangle, \langle m, n\rangle \in \mathbb{N} \times \mathbb{N}$,

$$[\langle k, l\rangle] + [\langle m, n\rangle] = [\langle k + m, l + n\rangle],$$
$$[\langle k, l\rangle] \cdot [\langle m, n\rangle] = [\langle k \cdot m + l \cdot n, k \cdot n + l \cdot m\rangle].$$

Ejemplo 407

Demostremos que el producto habitual en $\mathbb{Z}$ puede definirse como sigue, siendo $|\,|$ la función valor absoluto (*vid. infra* definición 17.86 [pág. 918 de esta edición]):

$$m \cdot n = \begin{cases} m \cdot n & \text{si} \quad m, n \in \mathbb{N} \\ -m \cdot |n| & \text{si} \quad m \in \mathbb{N} \wedge n \in \mathbb{Z}^- \\ |m| \cdot |n| & \text{si} \quad m, n \in \mathbb{Z}^- \end{cases}$$

Resolución.— En efecto, se deriva de la definición 15.5 (pág. 792 de esta edición):

$$\begin{aligned} m = [\langle m, 0\rangle] \in \mathbb{N} \wedge n = [\langle n, 0\rangle] \in \mathbb{N} \rightarrow m \cdot n &= [\langle m, 0\rangle] \cdot [\langle n, 0\rangle] \\ &= [\langle m \cdot n, 0\rangle] \\ &= m \cdot n; \\ m = [\langle m, 0\rangle] \in \mathbb{N} \wedge n = [\langle 0, |n|\rangle] \in \mathbb{Z}^- \rightarrow m \cdot n &= [\langle m, 0\rangle] \cdot [\langle 0, |n|\rangle] \\ &= [\langle 0, m \cdot |n|\rangle] \\ &= -m \cdot |n|; \\ m = [\langle 0, |m|\rangle] \in \mathbb{Z}^- \wedge n = [\langle 0, |n|\rangle] \in \mathbb{Z}^- \rightarrow m \cdot n &= [\langle 0, |m|\rangle] \cdot [\langle 0, |n|\rangle] \\ &= [\langle |m| \cdot |n|, 0\rangle] \\ &= |m| \cdot |n|. \end{aligned}$$ ■

§ 15.1.3 Orden

Definición 15.6 (Relaciones diádicas $\leq$ y $<$ en $(\mathbb{Z}; +)$).— Definimos en $(\mathbb{Z}; +)$ las relaciones diádicas $\leq$ y $<$:

0. $(\forall m, n \in \mathbb{Z})\ (m \leq n \leftrightarrow (\exists k \in \mathbb{N})(m + k = n))$;
1. $(\forall m, n \in \mathbb{Z})\ (m < n \leftrightarrow (\exists k \in \mathbb{N}^+)(m + k = n))$.

Teorema 15.12 (Interdefiniciones de $\leq$ y $<$)
Se satisface:

0. $(\forall m, n \in \mathbb{Z})\,(m \leq n \leftrightarrow m < n \lor m = n)$;
1. $(\forall m, n \in \mathbb{Z})\,(m < n \leftrightarrow m \leq n \land m \neq n)$.

Teorema 15.13 ($m + x = n$ resoluble en $\mathbb{Z}$)
Sean $m, n \in \mathbb{Z}$. La *ecuación* $m + x = n$ siempre tiene solución en $(\mathbb{Z}; +)$. La solución es $n - m$ y la llamamos *diferencia* de n y m.

Teorema 15.14 (Relación entre $\leq$, $<$ y la diferencia)
Se satisface:

0. $(\forall m, n \in \mathbb{Z})\,(m \leq n \leftrightarrow n - m \in \mathbb{N})$;
1. $(\forall m, n \in \mathbb{Z})\,(m < n \leftrightarrow n - m \in \mathbb{N}^+)$.

Teorema 15.15 (Orden total $\leq$ en $\mathbb{Z}$)
La relación diádica $\leq$ es un orden total en $(\mathbb{Z}; +)$.

Teorema 15.16 (Propiedades de $+$ y $\cdot$ en $\mathbb{Z}$)
En $(\mathbb{Z}; +, \cdot)$, la relación diádica $\leq$ también satisface las correspondientes propiedades de monotonía y cancelación con respecto a $+$ y $\cdot$:

0. $(\forall k, m, n \in \mathbb{Z})(m \leq n \leftrightarrow m + k \leq n + k)$; (monotonía para $+$)
1. $(\forall k, m, n \in \mathbb{Z})(k > 0 \rightarrow (m \leq n \leftrightarrow m \cdot k \leq n \cdot k))$; (monotonía para $\cdot$)
2. $(\forall k, m, n \in \mathbb{Z})(m + k = n + k \rightarrow m = n)$; (cancelación para $+$)
3. $(\forall k, m, n \in \mathbb{Z})(k \neq 0 \rightarrow (m \cdot k = n \cdot k \rightarrow m = n))$. (cancelación para $\cdot$)

Teorema 15.17 ($\mathbb{Z}$ no está bien ordenado por $\leq$)
La relación $\leq$ *no es un buen orden* en $(\mathbb{Z}; +)$, esto es, existen subconjuntos no vacíos de $\mathbb{Z}$ que no tienen primer elemento.

Demostración.— Obsérvese el propio conjunto $\mathbb{Z}$ o el conjunto de los números enteros pares; ninguno de ellos tiene primer elemento para la relación $\leq$. ■

Teorema 15.18 (Propiedad arquimediana en $\mathbb{Z}$)
$(\mathbb{Z}; +, \cdot; \leq)$ satisface la *propiedad arquimediana*[16], esto es, $(\forall m \in \mathbb{Z})(\forall n \in \mathbb{Z}^+)(\exists k \in \mathbb{N}^+)(m < k \cdot n)$.

[16] *Cfr. infra* definición 17.85 (pág. 917 de esta edición).

Teorema 15.19 (Algunas estructuras algebraicas presentes en $(\mathbb{Z}; +, \cdot; \leq)$)

0. $(\mathbb{Z}; +; \leq)$ es grupo conmutativo, (totalmente) ordenado;
1. $(\mathbb{Z}; \cdot; \leq)$ es monoide conmutativo, (totalmente) ordenado;
2. $(\mathbb{Z}; +, \cdot; \leq)$ es un anillo conmutativo, (totalmente) ordenado, unitario, íntegro y arquimediano.

§ 15.1.4 Axiomática «de tipo Peano» para $\mathbb{Z}$

Definición 15.7 (Axiomática «de tipo Peano» para $\mathbb{Z}$).— Además del sucesor de un número, puede considerarse su predecesor. Definimos así axiomáticamente $\mathbb{Z}$, en la línea de la definición de $\mathbb{N}$ de Peano, mediante el siguiente conjunto de axiomas:

I. $0 \in \mathbb{Z}$;

II. $(\forall n \in \mathbb{Z})(\text{pred}(n) \in \mathbb{Z} \wedge \text{suc}(n) \in \mathbb{Z})$;

III. $(\forall m, n \in \mathbb{Z})(\text{pred}(m) = \text{pred}(n) \to m = n)$;

IV. $(\forall m, n \in \mathbb{Z})(\text{suc}(m) = \text{suc}(n) \to m = n)$;

V. $((0 \in S) \wedge (\forall n \in S)(\text{pred}(a) \in S \wedge \text{suc}(m) \in S)) \to (\forall n \in \mathbb{Z})(n \in S)$; esto es, $S = \mathbb{Z}$.

§ 15.2 Números racionales

En este subcapítulo nos acercamos a la estructura del cuerpo conmutativo, (totalmente) ordenado, unitario, íntegro y arquimediano $(\mathbb{Q}; +, \cdot; \leq)$ de los números racionales.

§ 15.2.0 Un porqué

Aunque en $(\mathbb{Z}; +)$ sí tiene solución toda ecuación de la forma $m + x = n$, no ocurre lo propio en $(\mathbb{Z}; \cdot)$, por ejemplo, pensemos en la ecuación $3x = 7$.

Se puede remediar esta falta introduciendo los números racionales,

$$\mathbb{Q} = \{a/b : a \in \mathbb{Z} \wedge b \in \mathbb{Z}^+\},$$

de manera que ya sí es posible resolver la ecuación general

$$bx = a.$$

Así, todo número (racional), distinto de 0, tendrá simétrico respecto de la operación $\cdot$, en otras palabras, $(\mathbb{Q} \setminus \{0\}; \cdot)$ es grupo (conmutativo), y dicha ecuación tendrá solución única en $\mathbb{Q}$, a saber,

$$x = b^{-1} \cdot a.$$

§ 15.2.1 Definición constructiva de los números racionales

Consideramos en $\mathbb{Z} \times \mathbb{Z}^+$ la relación diádica

$$(\forall \langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z}^+)(\langle a, b\rangle E \langle c, d\rangle \leftrightarrow a \cdot d = b \cdot c).$$

Esta relación es de equivalencia. Por un lado, expresa todos los posibles cocientes, con denominador no nulo, que puede haber entre dos números enteros; por otro, clasifica estos cocientes. La clase de equivalencia $[\langle a, b\rangle]$, corresponde al cociente a/b, esto es, el número racional a/b no es más que dicha clase de equivalencia (a/b es la *representación normalizada* [o *irreducible*] de un número racional si a y b son coprimos). Por ello, el conjunto $\mathbb{Q}$, no es más que el conjunto cociente

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}^+ \big/ E.$$

§ 15.2.2 Operaciones

Definición 15.8 (Suma y producto de números racionales).— Definimos las operaciones diádicas suma y producto en $\mathbb{Q}$ en función de las de $\mathbb{Z}$ a través de la definición de dichas operaciones en $\mathbb{Z} \times \mathbb{Z}^+$, esto es, $\forall \langle a, b\rangle, \langle c, d\rangle \in \mathbb{Z} \times \mathbb{Z}^+$,

$$[\langle a, b\rangle] + [\langle c, d\rangle] = [(a \cdot d + b \cdot c, b \cdot d)],$$
$$[\langle a, b\rangle] \cdot [\langle c, d\rangle] = [(a \cdot c, b \cdot d)].$$

Con un proceder similar al visto en el ejemplo 407 (pág. 793 de esta edición), definimos las operaciones habituales en $\mathbb{Q}$.

§ 15.2.3 Relaciones

Entendiendo que el signo de un número racional es el de su numerador, $\operatorname{sgn}(a/b) = \operatorname{sgn}(a)$ —puesto que $\langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z}^+$—, ordenamos totalmente $\mathbb{Q}$ mediante la relación

$$(\forall p, q \in \mathbb{Q})\,(p \leq q \leftrightarrow \operatorname{sgn}(p - q) = -1)\,,$$

que también es posible definir como

$$(\forall a/b, c/d \in \mathbb{Q})\,(a/b \leq c/d \leftrightarrow a \cdot d \leq b \cdot c)\,.$$

Esta relación no es un buen orden; basta pensar en el primer elemento de $\mathbb{Q}$.

De la existencia del simétrico para todo racional no nulo, se derivan nuevas propiedades, por ejemplo,

$$(\forall p \in \mathbb{Q})(p \neq 0 \to |p^{-1}| = |p|^{-1}),$$

(propiedad que será también válida si $p \in \mathbb{R}$).

§ 15.2.4 Estructura

Teorema 15.20
$(\mathbb{Q}; +, \cdot; \leq)$ es denso, esto es, entre cualesquiera dos números racionales, p y q, hay otro número racional —la demostración es sencilla: por ejemplo, su punto medio, $(p+q)/2$—.

Observación 15.2.0.— Este hecho implica que en $(\mathbb{Q}; +, \cdot; \leq)$ no existen ni el predecesor ni el sucesor de ningún elemento para la relación $\leq$, pues si p fuese el predecesor de q, significaría que entre p y q no existiría ningún racional, en contra de la densidad de $(\mathbb{Q}; +, \cdot; \leq)$.

Sin embargo, sí que existen para otras relaciones que pudiesen definirse (recordemos, por ejemplo, el estudio de la cardinalidad numerable de $\mathbb{Q}$ y el buen orden que definimos en tal caso).

Notemos también que la densidad de $\mathbb{Q}$, esto es, el hecho de que entre dos números racionales cualesquiera exista siempre otro número racional, implica que entre dos números racionales cualesquiera hay un número infinito numerable de números racionales.

Teorema 15.21 (Propiedad arquimediana en $\mathbb{Q}$)
$(\mathbb{Q}; +, \cdot; \leq)$ satisface la *propiedad arquimediana*[17], esto es, $(\forall p \in \mathbb{Q})(\forall q \in \mathbb{Q}^+)(\exists k \in \mathbb{Z}^+)(p < k \cdot q)$.

Teorema 15.22
La estructura $(\mathbb{Q}; +, \cdot; \leq)$ es un cuerpo conmutativo, totalmente ordenado y arquimediano. En realidad, se puede demostrar que $(\mathbb{Q}; +, \cdot; \leq)$ es el menor cuerpo que extiende al anillo $(\mathbb{Z}; +, \cdot; \leq)$, estando determinado únicamente salvo isomorfismo.

Observación 15.2.1.— De manera similar al teorema anterior, puede completarse cualquier anillo de integridad (conmutativo) —generando su *cuerpo de cocientes*[18].

[17] *Cfr. infra* definición 17.85 (pág. 917 de esta edición).
[18] *Vid. infra* § 17.11.2 (pág. 910 de esta edición).

§ 15.3 Números reales

En este subcapítulo nos acercamos a la estructura del cuerpo conmutativo, (totalmente) ordenado, unitario, íntegro, arquimediano y completo $(\mathbb{R}; +, \cdot; \leq)$ de los números reales.

§ 15.3.0 Un porqué

Observemos que en $(\mathbb{Q}; +, \cdot; \leq)$ pueden efectuarse, sin ninguna restricción, sumas, diferencias, productos y cocientes. Entonces, ¿por qué necesitamos una extensión suya, el denominado sistema de números reales?

Una respuesta nos la proporciona el ejemplo 15.23 (pág. 798 de esta edición), que muestra la existencia de conjuntos de números racionales que no poseen supremo. Es decir, en $(\mathbb{Q}; +, \cdot; \leq)$ detectamos una cierta incompletitud de la estructura de orden.

§ 15.3.1 Construcción de los números reales

Veamos un procedimiento de construcción de $(\mathbb{R}; +, \cdot; \leq)$, completando la estructura de orden de $(\mathbb{Q}; +, \cdot; \leq)$, debido a DEDEKIND. Además de esta construcción, son clásicas las basadas en *cortaduras de* DEDEKIND, *sucesiones de* CAUCHY, o *intervalos encajados* (WEIERSTRASS).

Como comentamos en la observación 11.26.5 (pág. 656 de esta edición), todos los segmentos de $(\mathbb{Q}; +, \cdot; \leq)$ determinados por números racionales son secciones iniciales abiertas de $(\mathbb{Q}; +, \cdot; \leq)$, pero el recíproco, no es cierto, ya que por ejemplo, la sección inicial abierta $\mathbb{Q}^- \cup \{x \in \mathbb{Q} : x^2 < 2\}$ es un segmento, que no está determinado por ningún racional.

Así es.

Teorema 15.23
La sección inicial abierta $\mathbb{Q}^- \cup \{x \in \mathbb{Q} : x^2 < 2\}$ es un segmento, que no está determinado por ningún número racional.

Demostración.— En efecto, demostrar el enunciado equivale a demostrar que el conjunto $\{x \in \mathbb{Q} : x^2 < 2\}$ no posee supremo en $\mathbb{Q}$. Veámoslo. Creámonos que el supremo debe ser $\sqrt{2}$; bastará demostrar que $\sqrt{2} \notin \mathbb{Q}$. Razonemos por reducción al absurdo; supongamos que existen $p, q \in \mathbb{Z}^+$, tales que $\sqrt{2} = p/q$, siendo p/q una fracción irreducible. De aquí, $p^2 = 2q^2$, esto es, $p^2 \in$ Pares, de donde $p \in$ Pares: $(\exists k \in \mathbb{N} \setminus \{0\})(p = 2k)$, por lo que $p^2 = 2^2k^2 = 2q^2$, de donde, $q^2 = 2k^2$, por lo que q^2 es par y así q es par. Al ser $p, q \in$ Pares, p/q es reducible. He aquí el absurdo: «p/q es reducible e irreducible». ■

Pues bien, completaremos $(\mathbb{Q};\leq)$, a un conjunto ordenado que llamaremos $(\mathbb{R};\leq)$, de tal forma que en $(\mathbb{R};\leq)$ toda sección inicial abierta sea el segmento de un número de $\mathbb{R}$. De este modo, $\mathbb{R}$ es el conjunto de todas las secciones iniciales abiertas de $\mathbb{Q}$. Así, hemos definido los números reales como conjuntos particulares de números racionales y $(\mathbb{R};\leq)$ es un conjunto ordenado completo[19].

Definición 15.9 (Relación de orden constructiva).— Al quedar definido cada número real como un conjunto de números racionales, es posible definir una relación de orden en $\mathbb{R}$, en base a la inclusión de conjuntos (x e y son conjuntos):

$$(\forall x, y \in \mathbb{R})(x \leq y \leftrightarrow x \subseteq y).$$

Teorema 15.24
La relación anterior coincide con el orden habitual entre números reales (y por eso la notamos igual, $\leq$).

Teorema 15.25
La relación $\leq$ es de orden total, pero no es un buen orden.

Teorema 15.26
Toda sección inicial abierta de $(\mathbb{R},\leq)$, es el segmento de un número real.

Teorema 15.27
Todo conjunto acotado superiormente de números reales tiene supremo.

Observación 15.3.0.— Este último teorema, que es consecuencia del inmediatamente anterior, se corresponde al que, en la definición axiomática del sistema de números reales, se denomina *axioma del supremo*[20].

Definición 15.10.— Los números reales que no son segmentos de números racionales se llaman *números irracionales*.

§ 15.3.2 Definición axiomática de los números reales

Definición 15.11.— Llamamos sistema de números reales a la cuaterna $(\mathbb{R};+,\cdot;\leq)$, donde $+$ es una operación diádica que satisface:

0. $(\forall x, y \in \mathbb{R})(x + y = y + x)$, (conmutativa de $+$)

[19] *Vid. supra* definición 11.68 (pág. 657 de esta edición).
[20] *Vid. infra* definición 15.11 (pág. 799 de esta edición).

1. $(\forall x, y, z \in \mathbb{R})((x+y)+z = x+(y+z))$, (asociativa de $+$)

2. $(\exists 0 \in \mathbb{R})(\forall x \in \mathbb{R})(x+0 = x)$, ($0$ es el neutro de $+$ en $\mathbb{R}$)

3. $(\forall x \in \mathbb{R})(\exists(-x) \in \mathbb{R})(x+(-x) = 0)$, ($-x$ es el simétrico de x por $+$ en $\mathbb{R}$)

esto es, $(\mathbb{R};+)$ *es grupo conmutativo*;

$\cdot$ es otra operación diádica que satisface:

4. $(\forall x, y \in \mathbb{R})(x \cdot y = y \cdot x)$, (conmutativa de $\cdot$)

5. $(\forall x, y, z \in \mathbb{R})((x \cdot y) \cdot z = x \cdot (y \cdot z))$, (asociativa de $\cdot$)

6. $(\exists 1 \in \mathbb{R})(\forall x \in \mathbb{R})(x \cdot 1 = x)$, ($0$ es el neutro de $\cdot$ en $\mathbb{R}$)

7. $(\forall x \in \mathbb{R}^*)(\exists x^{-1} \in \mathbb{R})(x \cdot x^{-1} = 0)$, ($x^{-1}$ es el simétrico de x por $\cdot$ en $\mathbb{R}$)

esto es, $(\mathbb{R}^*;\cdot)$ *es grupo conmutativo*;

ambas operaciones, $+$ y $\cdot$ se relacionan:

8. $(\forall x, y, z \in \mathbb{R})(x \cdot (y+z) = x \cdot y + y \cdot z)$, ($\cdot$ se distribuye en $+$)

así, $(\mathbb{R};+,\cdot)$ *es cuerpo conmutativo*;

$\leq$ es una relación de orden total en $\mathbb{R}$ que satisface:

9. $(\forall x, y, z \in \mathbb{R})(x \leq y \to x+z \leq y+z)$, (monotonía de $+$ respecto de $\leq$)

10. $(\forall x, y \in \mathbb{R})(\forall z \in \mathbb{R}^+)(x \leq y \to x \cdot z \leq y \cdot z)$, (monotonía de $\cdot$ respecto de $\leq$)

por lo que $(\mathbb{R};+,\cdot;\leq)$ *es cuerpo conmutativo totalmente ordenado*.

Pero aún queda un detalle. $(\mathbb{Q};+,\cdot;\leq)$ también es un cuerpo conmutativo totalmente ordenado. Esto quiere decir que no es posible definir $\mathbb{R}$ sólo con las propiedades anteriores, pues también incluiría la definición de $\mathbb{Q}$. Lo que realmente distingue a $\mathbb{R}$ de $\mathbb{Q}$, es el hecho de satisfacer la propiedad que se conoce como *axioma del supremo* (o, sinónimamente, *axioma del extremo superior* o *axioma de completitud*):

11. $(\forall A \subset \mathbb{R}, A \neq \emptyset)(A \text{ acotado superiormente} \to \exists \sup(A,\mathbb{R}))$. (axioma del supremo)

En la definición axiomática es este axioma el que aporta la completitud a la estructura de orden. En definitiva, y a diferencia de $(\mathbb{Q};+,\cdot;\leq)$, $(\mathbb{R};+,\cdot;\leq)$ *es un cuerpo conmutativo ordenado completo*.

Observación 15.3.1.— Como consecuencia inmediata del axioma del supremo, en $(\mathbb{R};+,\cdot;\leq)$, todo conjunto no vacío y acotado inferiormente tiene ínfimo. En realidad, ésta —que pudiésemos llamar *propiedad de existencia del ínfimo*— y el axioma del supremo, como afirmaciones, son equivalentes. En efecto, tal equivalencia se desprende de que: primero, ser A no vacío y acotado superiormente equivale a ser $-A = \{-x : x \in A\}$ no vacío y acotado inferiormente, y segundo,

que exista $\sup(A, \mathbb{R})$ equivale a que exista $\inf(A, \mathbb{R})$. Consecuentemente, en vez del axioma del supremo pudiésemos adoptar en la definición axiomática de $\mathbb{R}$ como axioma n.º 11 la propiedad de existencia del ínfimo, y con ella obtendríamos como teorema la existencia del supremo.

Teorema 15.28 (De los intervalos encajados)
Toda sucesión de intervalos cerrados, acotados y encajados $I_0 \supseteq I_1 \supseteq I_2 \supseteq \ldots$, es tal que la intersección de todos ellos es no vacía.

Demostración.— Por el axioma del supremo existe el supremo s de los extremos izquierdos de los intervalos I_j y por la propiedad de existencia del ínfimo existe el ínfimo i de los extremos derechos de los intervalos I_j. Parece trivial que $s \leq i$ y que $[s, i] \subseteq I_j$, para todo j. Observemos que si las longitudes de los I_j progresan hacia cero, $s = i$ y la intersección de todos ellos es precisamente dicho número $s(= i)$. ■

Observación 15.3.2.— Igual que con la propiedad de existencia del ínfimo ocurre con la propiedad de los intervalos encajados. Si en vez del axioma del supremo adoptásemos como axioma esta propiedad, obtendríamos como teorema la existencia del supremo.

Teorema 15.29 (Propiedad arquimediana en $\mathbb{R}$)
$(\mathbb{R}; +, \cdot; \leq)$ satisface la *propiedad arquimediana*[21], esto es, $(\forall r \in \mathbb{R})(\forall s \in \mathbb{R}^+)(\exists k \in \mathbb{Z}^+)(r < k \cdot s)$.

Ejemplo 408

Demostremos que todo intervalo (a, b) de números reales, no vacío, contiene algún número racional y algún número irracional.

Resolución.— Lo demostramos por dos vías.

Vía 0.

Por un lado, supondremos conocido que si q es racional y r es irracional, entonces $q + r$ y $q \cdot r$ son irracionales; por otro, usaremos la propiedad arquimediana[22], en dos ocasiones, al afirmar que $\exists n$ tal que $n(b - a) > 1$ (en la propiedad arquimediana, $s \hookleftarrow 1$, $r \hookleftarrow b - a$) y al afirmar que $\exists n$ tal que $n(b - a) > 2$ (en la propiedad arquimediana, $s \hookleftarrow 2$, $r \hookleftarrow b - a$).

Nuestro primer objetivo consiste en encontrar un número racional m/n tal que $a < m/n < b$. Por un lado, observemos que si n es tal que $n(b-a) > 1$, entonces $1/n < b-a$; por otro, si $t = \lfloor na \rfloor$, entonces, por definición de la función suelo, $t \leq na < t + 1$, de donde $t/n \leq a < (t+1)/n =$

[21] *Cfr. infra* definición 17.89 (pág. 920 de esta edición).
[22] *Cfr. supra* teorema 15.29 (pág. 801 de esta edición).

$t/n + 1/n < a + (b - a) = b$, por lo que hemos obtenido un número racional entre a y b, a saber, $(t+1)/n$, esto es,

$$\frac{\lfloor na \rfloor + 1}{n},$$

siendo n tal que $1 < n(b-a)$.

Nuestro segundo objetivo es encontrar un número irracional entre a y b. Sigamos un razonamiento similar al anterior. Por un lado, si n es tal que $n(b-a) > 2$, entonces $2/n < b - a$; por otro, si $t = \lfloor na \rfloor$, entonces, por definición de la función suelo, $t \leq na < t+1$, de donde $t/n \leq a < (t+1)/n < (t+\sqrt{2})/n < (t+2)/n = t/n + 2/n < a + (b-a) = b$, por lo que hemos obtenido un número irracional en (a, b), a saber, $(t+\sqrt{2})/n$, esto es,

$$\frac{\lfloor na \rfloor + \sqrt{2}}{n},$$

siendo n tal que $2 < n(b-a)$. □

Vía 1.

La aplicación $f(x) = a - (a-b)x$ es una biyección de $(0,1)$ en (a,b) que transforma racionales en racionales e irracionales en irracionales (supondremos conocido que la suma y el producto de racionales es racional y que si q es racional y r es irracional, entonces $q + r$ y $q \cdot r$ son irracionales). Sabemos que $\sqrt{2}$ es irracional y trivialmente, $1/2 \in (0,1) \cap \mathbb{Q}$ y $1/\sqrt{2} \in (0,1) \cap (\mathbb{R} \setminus \mathbb{Q})$, por lo que por lo anterior, $f(1/2) = a - (a-b)/2 \in (a,b) \cap \mathbb{Q}$ y $f(1/\sqrt{2}) = a - (a-b)/\sqrt{2} \in (a,b) \cap (\mathbb{R} \setminus \mathbb{Q})$. ■

Ejemplo 409

Demostremos que todo intervalo (a, b) de números reales, no vacío, contiene un número infinito de números racionales y un número infinito de números irracionales.

Resolución.— Esto es consecuencia inmediata del ejemplo 408 (pág. 801 de esta edición). Veamos, por ejemplo, que contiene un número infinito de racionales. En dicho ejemplo hemos demostrado que todo intervalo (x, y) no vacío contiene un número racional (todo intervalo, ésa es la clave). Sea q_0 tal número racional, entonces, por el ejemplo 408 (pág. 801 de esta edición) existen $q_1, q_2 \in \mathbb{Q}$, $q_1 \in (a, q_0)$ y $q_2 \in (q_0, b)$, de donde, de nuevo por dicho ejemplo existen $q_3, q_4, q_5, q_6 \in \mathbb{Q}$, $q_3 \in (a, q_1)$, $q_4 \in (q_1, q_0)$, $q_5 \in (q_0, q_2)$ y $q_6 \in (q_2, b)$, y así sucesivamente, de manera que obtenemos un subconjunto infinito de racionales $\{q_0, q_1, q_2, q_3, q_4, q_5, q_6, \ldots\} \subseteq (a, b)$.

La demostración de que contiene un número infinito de irracionales es similar. ■

Observación 15.3.3.— Destacable es que los números infinitos de los que hablamos son distintos. Debido a que el número total de racionales es numerable y a que el cardinal del intervalo de números reales es infinito no numerable, *todo intervalo de números reales contiene un número infinito numerable de racionales y un número infinito no numerable de números irracionales.*

§ 15.4 Bibliografía

[147] Herbert Bruce ENDERTON. *Elements of Set Theory*. Academic Press, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1977.

[148] Karel HRBACEK y Thomas J. JECH. *Introduction to set theory*. Monographs and textbooks in pure and applied mathematics. Marcel Dekker, Nueva York, Nueva York (US-NY), Estados Unidos de América, 3.ª ed., 1999.

[189] Carlos IVORRA CASTILLO. *Álgebra*. Autoedición, Valencia, Comunidad Valenciana [ES-VC], España, 2022. https://www.uv.es/ivorra/Libros/Al.pdf (accedido el 26.1.2024). ©gratisOA.

CAPÍTULO 16

Lógica inductiva

Dos es casualidad, tres, un patrón.

(Paremia anónima).

Al estudiar lógica de primer orden vimos la inducción como una inferencia. En este capítulo profundizamos en ella, estudiando cómo la estrategia de demostración por inducción se fundamenta en un buen orden (total) (inducción débil, inducción fuerte o inducción estructural) o bien en un orden bien fundado (esto es, un buen orden parcial) (inducción noetheriana). La inducción de CAUCHY puede basarse en cualquiera de ellos, si bien en el ejemplo de aplicación que veremos será en un orden total.

§ 16.0 Inducción débil

Teorema 16.0 (Inducción débil para $\mathbb{N}$)
Se satisface:

$$\begin{aligned} \mathrm{ID}_0 &\leftrightharpoons P(0); \\ \mathrm{ID}_1 &\leftrightharpoons (\forall k \in \mathbb{N})(P(k) \to P(k+1)); \\ \mathrm{ID}_0 \wedge \mathrm{ID}_1 &\vdash \forall n \in \mathbb{N}, P(n). \end{aligned}$$

Que en formato de regla se expresa así:

$$\frac{P(0) \qquad (\forall k \in \mathbb{N})(P(k) \to P(k+1))}{\forall n \in \mathbb{N}, P(n)}$$

Se conoce como *caso base* (ID_0) a $P(0)$, *paso inductivo (débil)* (ID_1) a $(\forall k \in \mathbb{N})(P(k) \to P(k+1))$, *hipótesis inductiva (débil)* a $P(k)$ y *tesis inductiva (débil)* a $P(k+1)$.

Observación 16.0.0.— Quien dice $\langle k, k+1\rangle$, dice $\langle k-1, k\rangle$, esto es, pudiésemos haberla enunciado:

$$\begin{aligned} \mathrm{ID}_0 &\leftrightharpoons P(0); \\ \mathrm{ID}_1 &\leftrightharpoons (\forall k \in \mathbb{Z}^+)(P(k-1) \to P(k)); \\ \mathrm{ID}_0 \wedge \mathrm{ID}_1 &\vdash \forall n \in \mathbb{N}, P(n). \end{aligned}$$

Ejemplo 410

Demostremos que $\forall n \in \mathbb{N}, 2^n > n$.

[SEL 4:14]. *Cfr.* Rosen [151]: § 3.3 Inducción matemática, ejemplo 2 (pág. 225).

Resolución.— Notando «$2n > n$» por $P(n)$, lo que nos proponemos es demostrar que $\forall n \in \mathbb{N}, P(n)$. Para ello, apliquemos el teorema 16.0 (pág. 805 de esta edición):

Caso base (ID_0).— Si $n = 0$, $2^0 = 1 > 0$, por lo que $P(0)$ es cierta.

Paso inductivo (ID_1).— Supongamos $P(k)$ y demostremos $P(k+1)$, esto es, supongamos que $2^k > k$ y demostremos $2^{k+1} > k+1$; como $2^{k+1} = 2 \cdot 2^k > 2 \cdot k = k + k > k+1$, se tiene $P(k+1)$.

Conclusión ($\mathrm{ID}_0 \wedge \mathrm{ID}_1$).— Como se satisfacen el caso base y el paso inductivo, entonces del teorema 16.0 (pág. 805 de esta edición) de inducción débil se sigue lo buscado, a saber, que $\forall n \in \mathbb{N}, 2^n > n$. ■

Ejemplo 411 Cardinal del conjunto potencia

Demostremos que si $|X| = n$, entonces $|2^X| = 2^n$.

[Cubit 53].

Resolución.— Notando «$|X| = n \to |2^X| = 2^n$» por $P(n)$, lo que nos proponemos es demostrar que $\forall n \in \mathbb{N}, P(n)$. Para ello, apliquemos el teorema 16.0 (pág. 805 de esta edición):

Caso base (ID_0).— Si $n = 0$, $X = \emptyset$ y $2^\emptyset = \{\emptyset\}$ (el único subconjunto de $\emptyset$ es $\emptyset$), por lo que $|2^X| = 1 = 2^0$ y por tanto, $P(0)$ es cierta.

Paso inductivo (ID_1).— Supongamos $P(k)$ y demostremos $P(k+1)$, esto es, supongamos que para todo conjunto con $n = k$ elementos, su conjunto potencia tenga 2^k elementos; para ello, consideremos un conjunto X con $n = k + 1$ elementos; quitémosle uno, llamémoslo x, entonces el conjunto restante $X \setminus \{x\}$ tiene k elementos y su conjunto potencia 2^k; estos 2^k elementos son todos los subconjuntos de X que no contienen a x; el número de subconjuntos de X que contienen a x es fácil hallarlo, son todos aquéllos subconjuntos de X que no contienen a x, introduciendo x en ellos, o sea, también 2^k; por tanto, 2^X tiene $2^k + 2^k = 2(2^k) = 2^{k+1}$ elementos, esto es, se tiene $P(k+1)$.

Conclusión ($ID_0 \wedge ID_1$).— Como se satisfacen el caso base y el paso inductivo, entonces del teorema 16.0 (pág. 805 de esta edición) de inducción débil se sigue lo buscado, a saber, que $(\forall n \in \mathbb{N})\,(|X| = n \to |2^X| = 2^n)$. ■

Teorema 16.1 (Inducción débil para $\mathbb{N} \setminus \{0\}$)

Se satisface:

$$\begin{aligned} ID_0 &\leftrightharpoons P(1); \\ ID_1 &\leftrightharpoons (\forall k \in \mathbb{N} \setminus \{0\})(P(k) \to P(k+1)); \\ ID_0 \wedge ID_1 &\vdash \forall n \in \mathbb{N} \setminus \{0\}, P(n). \end{aligned}$$

Que en formato de regla se expresa así:

$$\frac{P(1) \qquad (\forall k \in \mathbb{N} \setminus \{0\})(P(k) \to P(k+1))}{\forall n \in \mathbb{N} \setminus \{0\}, P(n)}$$

Ejemplo 412

Demostremos que $\forall n \in \mathbb{Z}^+, 1 + 3 + 5 + \ldots + (2n - 1) = n^2$.

[SEL 4:14]. *Cfr.* ROSEN [151]: § 3.3 Inducción matemática, ejemplo 1 (pág. 224).

Resolución.— Notando «$1 + 3 + 5 + \ldots + (2n - 1) = n^2$» por $P(n)$, lo que nos proponemos es demostrar que $\forall n \in \mathbb{Z}^+, P(n)$. Para ello, apliquemos el teorema 16.1 (pág. 806 de esta edición):

Caso base (ID_0).— Si $n = 1$, entonces $1 = 1^2$, de donde $P(1)$ es cierta.

Paso inductivo (ID_1).— Supongamos $P(k)$ y demostremos $P(k + 1)$, esto es, supongamos que $1 + 3 + \ldots + (2k - 1) = k^2$ y demostremos que $1 + 3 + \ldots + (2(k + 1) - 1) = (k + 1)^2$; en efecto, $1 + 3 + \ldots + (2k - 1) + (2(k + 1) - 1) = k^2 + (2(k + 1) - 1) = (k + 1)^2$, esto es, $P(k + 1)$.

Conclusión ($ID_0 \wedge ID_1$).— Como se satisfacen el caso base y el paso inductivo, entonces del teorema 16.1 (pág. 806 de esta edición) de inducción débil se sigue lo buscado, a saber, que $\forall n \in \mathbb{Z}^+, 1 + 3 + 5 + \ldots + (2n - 1) = n^2$. ■

Ejemplo 413

El conjunto de todas las potencias positivas de 2 y el conjunto de todos los múltiplos positivos de 3 son disjuntos.

Resolución.— Hagamos la traducción inversa. Debemos demostrar que si $A = \{x : x > 0 \wedge \exists k \in \mathbb{N}, x = 2^k\}$ y $B = \{x : x > 0 \wedge \exists k \in \mathbb{N}, x = 3k\}$, entonces $A \cap B = \emptyset$. Notando «$\forall p, q \in \mathbb{Z}^+, 2^p \neq 3q$» por $P(p)$, debemos demostrar que $\forall p \in \mathbb{Z}^+, P(p)$. Hagámoslo por inducción débil sobre p (*cfr. infra* teorema 16.1 [pág. 806 de esta edición]):

Caso base (ID_0).— Analicemos uno o más casos básicos: si $p = 1$, entonces $\forall q \in \mathbb{Z}^+, 2^1 \neq 3q$ (el único q posible sería $2/3 \notin \mathbb{Z}^+$); similarmente, si $p = 2$, entonces $\forall q \in \mathbb{Z}^+, 2^2 \neq 3q$ (el único q posible sería $4/3 \notin \mathbb{Z}^+$), por lo que $P(1)$ es cierta.

Paso inductivo (ID_1).— Supongamos $P(k)$ y demostremos $P(k+1)$, esto es, supongamos que $\forall q \in \mathbb{Z}^+, 2^p \neq 3q$ (la *hipótesis inductiva* [HI]) y demostremos que $\forall q \in \mathbb{Z}^+, 2^{p+1} \neq 3q$ (la *tesis inductiva* [TI]); razonemos *por contraposición*: supongamos que TI no es cierta, esto es, que $\exists q' \in \mathbb{Z}^+$ tal que $2^{p+1} = 3q'$, de aquí, q' debe ser múltiplo de 2 (al no serlo 3) y, además, $2^p = 3q'/2$, es decir, $2^p = 3k$ (con $k \in \mathbb{Z}^+$), por lo que $\exists q(= k) \in \mathbb{Z}^+, 2^p = 3q$, es decir, HI es falsa.

Conclusión ($ID_0 \wedge ID_1$).— Como se satisfacen el caso base y el paso inductivo, entonces del teorema 16.1 (pág. 806 de esta edición) de inducción débil se sigue lo buscado, a saber, que $\forall p, q \in \mathbb{Z}^+, 2^p \neq 3q$. ■

Teorema 16.2 (Inducción débil para $\mathbb{N} \setminus \{0, 1, 2, \ldots, m\}$)
Se satisface:

$$\begin{aligned} \mathrm{ID}_0 &\leftrightharpoons P(m+1); \\ \mathrm{ID}_1 &\leftrightharpoons (\forall k \in \mathbb{N} \setminus \{0, 1, 2, \ldots, m\})(P(k) \to P(k+1)); \\ \mathrm{ID}_0 \wedge \mathrm{ID}_1 &\vdash \forall n \in \mathbb{N} \setminus \{0, 1, 2, \ldots, m\}, P(n). \end{aligned}$$

Que en formato de regla se expresa así:

$$\frac{P(m+1) \qquad (\forall k \in \mathbb{N} \setminus \{0, 1, 2, \ldots, m\})(P(k) \to P(k+1))}{\forall n \in \mathbb{N} \setminus \{0, 1, 2, \ldots, m\}, P(n)}$$

Ejemplo 414

Demostremos que $\forall n \in \mathbb{N} \setminus \{0, 1, 2, 3\}, n^2 > 3n$.

[Cubit 56].

Resolución.— Notando «$n^2 > 3n$» por $P(n)$, lo que nos proponemos es demostrar que $\forall n \in \mathbb{N} \setminus \{0, 1, 2, 3\}, P(n)$. Para ello, apliquemos el teorema 16.2 (pág. 808 de esta edición):

Caso base (ID_0).— Si $n = 4$, entonces $42 = 16 > 12 = 3 \cdot 4$, por lo que $P(4)$ es verdadera.

Paso inductivo (ID_1).— Supongamos $P(k)$ y demostremos $P(k+1)$, esto es, supongamos que $k^2 > 3 \cdot k$ y demostremos $(k+1)^2 > 3 \cdot (k+1)$; en efecto, como $(k+1)^2 = k^2 + 2k + 1 \overset{P(k)}{>} 3k + 2k + 1 \overset{k \geq 4}{\geq} 3k + 8 + 1 > 3k + 3 = 3 \cdot (k+1)$;

Conclusión ($\mathrm{ID}_0 \wedge \mathrm{ID}_1$).— Como se satisfacen el caso base y el paso inductivo, entonces del teorema 16.2 (pág. 808 de esta edición) de inducción débil se sigue lo buscado, a saber, que $\forall n \in \mathbb{N} \setminus \{0, 1, 2, 3\}, n^2 > 3n$. ■

Ejemplo 415

Si sólo se dispone de sellos de 3 céntimos y de 5 céntimos, es posible formar cualquier franqueo de 8 o más céntimos.

[Cubit 57], [EFE 7.7.2021:3] (con 3 y 7 céntimos, un franqueo de 12 o más), [EFO 20.5.2022:4a], [SEL 4:12a] (con 4 y 5 céntimos, un franqueo de 12 o más). *Cfr.* HAMMACK [122]: § 10.2 *Proofs by Strong Induction*, Proposición (págs. 187–188).

Resolución.— Formalmente, tenemos que demostrar que $\forall n \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}$, $P(n)$, donde $P(n)$ es la afirmación «puede formarse un franqueo de n céntimos sólo con sellos de 3 y de 5 céntimos». Para ello, apliquemos el teorema 16.2 (pág. 808 de esta edición) (inducción débil):

Caso base (ID_0).— En la base de la inducción, analizamos la veracidad de cuantos casos, en número finito, estimemos oportunos: $8 = 1 \cdot 3 + 1 \cdot 5$, $9 = 3 \cdot 3 + 0 \cdot 5$, $10 = 0 \cdot 3 + 2 \cdot 5$, $11 = 2 \cdot 3 + 1 \cdot 5$, $12 = 4 \cdot 3 + 0 \cdot 5$, etc.

Paso inductivo (ID_1).— En la inducción propiamente, hemos de asegurar la exhaustividad de la lista de posibilidades. Lo aseguramos haciendo una partición en una situación y su contraria. Así, en un franqueo determinado mayor o igual de 8 cts. con sellos de 3 y 5 cts. puede ocurrir:

I. que al menos incluya un sello de 3 cts. y al menos un sello de 5 cts., o

II. lo contrario[°], esto es, que no incluya ningún sello de 3 cts. o que no incluya ningún sello de 5 cts., distinguiéndose en este caso sólo dos situaciones [por definición de la disyunción y porque no puede suceder a la vez que no incluya de 3 ni de 5 cts., so pena de no existir franqueo formado sólo con sellos de 3 y 5 cts.]:

   0. que no incluya de 3 cts. —por lo que al menos incluye dos de 5 cts. [como mínimo el franqueo es de 10 cts.]—;

   1. que no incluya de 5 cts. —por lo que al menos hay tres de 3 cts. [como mínimo el franqueo es de 9 cts.]—.

Demostrar que se satisface el paso inductivo de la inducción débil no es difícil; en las posibilidades anteriores:

I. si al menos incluye un sello de 3 cts. y al menos un sello de 5 cts., se sustituye uno de 3 cts. y uno de 5 cts. —un total de 8 cts.— por tres de 3 cts. —un total de 9 cts.—;

II. si no incluye ningún sello de 3 cts. o no incluye ningún sello de 5 cts.:

   0. se sustituye uno de 5 cts. por dos de 3 cts. —un total de 6 cts.—;

   1. se sustituyen tres de 3 cts. —un total de 9 cts.— por dos de 5 cts. —un total de 10 cts.—.

Conclusión ($\mathrm{ID}_0 \wedge \mathrm{ID}_1$).— Como se satisfacen el caso base y el paso inductivo, entonces del teorema 16.2 (pág. 808 de esta edición) de inducción débil se sigue lo buscado, a saber, que $\forall n \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}$ se satisface la afirmación $P(n)$. ■

[°] Si $Rx \leftrightharpoons x$ es un sello de 3 cts. y $Sx \leftrightharpoons x$ es un sello de 5 cts. y el dominio de interpretación es el franqueo dado, entonces «el franqueo al menos incluye un sello de 3 cts. y al menos un sello de 5 cts.» se formaliza en LPO por $\exists x Rx \wedge \exists y Sy$, o equivalentemente (✍) por $\exists x \exists y (Rx \wedge Sy)$, siendo su negación (✍) $\forall x \forall y (\neg Rx \vee \neg Sy)$, o equivalentemente (✍) $\forall x \neg Rx \vee \forall y \neg Sy$, esto es, «el franqueo no incluye ningún sello de 3 cts. o no incluye ningún sello de 5 cts.».

Observación 16.0.1.— Para saber más, pudiésemos consultar, por ejemplo, el artículo Problema de la moneda, en la Wikipedia en español[1] y leer en él cómo dados dos enteros positivos x e y, el mayor número no representable por una combinación lineal de coeficientes no negativos $ax+by$ es $xy-x-y$.

Por ejemplo, con $x=3$ e $y=5$ (ejemplo anterior), el mayor número no representable es $3\cdot 5-3-5=7$, en otras palabras, a partir de 8 (incluido) sí es posible; por poner otro ejemplo, siendo $x=4$ e $y=5$, el mayor número no representable es $4\cdot 5-4-5=11$, en otras palabras, a partir de 12 (incluido) sí es posible.

§ 16.1 Inducción fuerte

Teorema 16.3 (Inducción fuerte para $\mathbb{N}$)
Se satisface:

$$\begin{aligned} \mathrm{IF}_0 &\leftrightharpoons P(0);\\ \mathrm{IF}_1 &\leftrightharpoons (\forall k\in\mathbb{N})(P(0)\wedge P(1)\wedge\ldots\wedge P(k)\to P(k+1));\\ \mathrm{IF}_0\wedge\mathrm{IF}_1 &\vdash \forall n\in\mathbb{N}, P(n). \end{aligned}$$

Que en formato de regla se expresa así:

$$\frac{P(0)\qquad (\forall k\in\mathbb{N})(P(0)\wedge P(1)\wedge\ldots\wedge P(k)\to P(k+1))}{\forall n\in\mathbb{N}, P(n)}$$

Se conoce como *caso base* (IF_0) a $P(0)$, *paso inductivo fuerte* (IF_1) a $(\forall k\in\mathbb{N})(P(0)\wedge P(1)\wedge\ldots\wedge P(k)\to P(k+1))$, *hipótesis inductiva fuerte* a $P(0)\wedge P(1)\wedge\ldots\wedge P(k)$ y *tesis inductiva fuerte* a $P(k+1)$.

Observación 16.1.0.— Quien dice $\langle k,k+1\rangle$, dice $\langle k-1,k\rangle$, esto es, pudiésemos haberla enunciado:

$$\begin{aligned} \mathrm{IF}_0 &\leftrightharpoons P(0);\\ \mathrm{IF}_1 &\leftrightharpoons (\forall k\in\mathbb{Z}^+)(P(0)\wedge P(1)\wedge\ldots\wedge P(k-1)\to P(k));\\ \mathrm{IF}_0\wedge\mathrm{IF}_1 &\vdash \forall n\in\mathbb{N}, P(n). \end{aligned}$$

La inducción fuerte también es válida en los casos comentados anteriormente, esto es, para $\mathbb{N}\setminus\{0\}$ y para $\mathbb{N}\setminus\{0,1,2,\ldots,m\}$. Un ejemplo de este último, el siguiente.

[1] *Vid*. https://es.wikipedia.org/wiki/Problema_de_la_moneda.

Ejemplo 416

Demostremos que «$n \in \mathbb{N} \setminus \{0, 1\}$ es o bien un número primo, o bien un producto de dos o más números primos».

[Cubit 60], [SEL 4:18]. *Cfr.* Rosen [151]: § 3.3 Inducción matemática, ejemplo 14 (págs. 232–233). *Vid. infra* el Teorema fundamental de la aritmética en su contexto: teorema 18.17 (pág. 959 de esta edición).

Resolución.— Siendo $P(n) \coloneqq$ «n es o bien un número primo, o bien un producto de dos o más números primos», lo que nos proponemos es demostrar que $\forall n \in \mathbb{N} \setminus \{0, 1\}, P(n)$. Para ello, apliquemos el teorema 16.3 (pág. 810 de esta edición) de inducción fuerte:

Caso base (IF_0).— Como 2 es primo, $P(2)$ es verdadera.

Paso inductivo fuerte (IF_1).— Supongamos $P(0), P(1), \ldots, P(k)$ y demostremos $P(k+1)$, esto es, supongamos que dado $k \in \mathbb{N}$, todo $r \leq k$ es o bien primo, o bien producto de dos o más primos; ¿qué pasa con $k+1$?; $k+1$ puede ser primo o no serlo; si lo es, ya está demostrada la validez del paso inductivo fuerte; si no lo es, $\exists r, s \leq k$ tales que $k+1 = r \cdot s$ (r y s no pueden ser mayores que k, pues si uno fuese $k+1$, el otro sería 1, pero suponemos que $n \geq 2$; por la hipótesis fuertemente inductiva, r es primo o producto de primos y también s, de donde $k+1$ es producto de dos o más primos.

Conclusión ($IF_0 \wedge IF_1$).— Como se satisfacen el caso base y el paso inductivo fuerte, entonces del teorema 16.3 (pág. 810 de esta edición) de inducción fuerte se sigue lo buscado, a saber, que $\forall n \in \mathbb{N} \setminus \{0, 1\}, P(n)$. ■

Actividad 16.0

¿Nos atrevemos a demostrar que salvo el orden de los factores, dicha factorización es única?

[Cubit 61]. *Vid. infra* el Teorema fundamental de la aritmética en su contexto: teorema 18.17 (pág. 959 de esta edición).

Ejemplo 417

Si sólo se dispone de sellos de 3 céntimos y de 5 céntimos, es posible formar cualquier franqueo de 8 o más céntimos.

[Cubit 58], [EFO 20.5.2022:4b], [EFE 7.7.2021:3] (con 3 y 7 céntimos, un franqueo de 12 o más), [SEL 4:12b] (con 4 y 5 céntimos, un franqueo de 12 o más). *Cfr.* Hammack [122]: § 10.2 *Proofs by Strong Induction*, Proposición (págs. 187–188).

Resolución.— Siendo $P(n) \fallingdotseq$ «puede formarse un franqueo de n céntimos sólo con sellos de 3 y de 5 céntimos», lo que nos proponemos es demostrar que $\forall n \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}, P(n)$. Para ello, apliquemos el teorema 16.3 (pág. 810 de esta edición) de inducción fuerte:

Caso base (IF_0).— El paso base de la inducción fuerte es común con la inducción débil y éste lo analizamos en el ejemplo 415 (pág. 808 de esta edición).

Paso inductivo fuerte (IF_1).— Sea $k \geq 10$ y supongamos que $\forall m \in \mathbb{N}$, con $8 \leq m \leq k$, es posible formar un franqueo de m cts. sólo con sellos de 3 y 5 cts., esto es, supongamos ciertas $P(8)$, $P(9), \ldots, P(k)$. Dado k, basta entonces añadir un sello de 3 cts. al franqueo de $k-2$ cts. [que por ser $k \geq 10$, $k-2 \geq 8$] para obtener un franqueo de $k+1$ cts.

Conclusión ($IF_0 \wedge IF_1$).— Como se satisfacen el caso base y el paso inductivo fuerte, entonces del teorema 16.3 (pág. 810 de esta edición) de inducción fuerte se sigue lo buscado, a saber, que $\forall n \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}$ se satisface la afirmación $P(n)$. ∎

Ejemplo 418

Si x es una palabra de $\{0, 1\}^*$, entonces $0x \neq x1$.

Resolución.— Siendo $P(n) \fallingdotseq$ «si x es una palabra de $\{0, 1\}^*$ y $|x| = n$, entonces $0x \neq x1$», lo que nos proponemos es demostrar que $\forall n \in \mathbb{N}, P(n)$. Para ello, apliquemos el teorema 16.3 (pág. 810 de esta edición) de inducción fuerte:

Caso base (IF_0).— Si n es 0, $0\varepsilon = 0 \neq 1 = \varepsilon 1$.

Paso inductivo fuerte (IF_1).— Supongamos que $\forall m \in \mathbb{N}, m < k$, si x es una palabra de $\{0, 1\}^*$ y $|x| = m$, entonces $0x \neq x1$, esto es, supongamos ciertas $P(1), P(2), \ldots, P(k-1)$. Supongamos ahora que $|x| = k$, esto es, demostremos que si $|x| = k$, $0x \neq x1$; utilizamos reducción al absurdo para ello: si $0x = x1$, entonces la primera letra de x es 0 y su última letra es 1, esto es, existe una palabra u tal que $x = 0u1$, es decir, sustituyendo, tal que $00u1 = 0u11$, o sea, tal que $0u = u1$, pero como $|u| < |x|$, por la hipótesis de inducción, $0u \neq u1$; por lo que hemos llegado a la contradicción $(0u = u1) \wedge (0u \neq u1)$; por lo tanto, por reducción al absurdo: si $|x| = k$, $0x \neq x1$, esto es, la tesis de inducción.

Conclusión ($IF_0 \wedge IF_1$).— Como se satisfacen el caso base y el paso inductivo fuerte, entonces del teorema 16.3 (pág. 810 de esta edición) de inducción fuerte se sigue lo buscado, a saber, que $\forall n \in \mathbb{N}$ se satisface la afirmación $P(n)$.[2] ∎

[2] *Vid. supra* una demostración por reducción al absurdo en el ejemplo 251 (p. 479).

Ejemplo 419

Sea $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$ definida por $f(n) = n/2$ si n es par y $f(n) = n + 1$ si n es impar; demostremos por inducción fuerte que para todo entero positivo n, la iteración de $f(n)$ (esto es, $f(n), f(f(n)), f(f(f(n))), \ldots$ —que abreviamos por $f^{(1)}(n), f^{(2)}(n), f^{(3)}(n), \ldots$—) toma el valor 1 en algún momento. (Por ejemplo: $23 \mapsto 24 \mapsto 12 \mapsto 6 \mapsto 3 \mapsto 4 \mapsto 2 \mapsto 1$).

Resolución.— Siendo $P(n) \leftrightharpoons$ «existe $h \in \mathbb{Z}^+$ tal que $f^{(h)}(n) = 1$», lo que nos proponemos es demostrar que $\forall n \in \mathbb{Z}^+, P(n)$. Para ello, apliquemos el teorema 16.3 (pág. 810 de esta edición) de inducción fuerte:

Caso base (IF_0).— Si n es 1, h es 2, pues $f^{(2)}(1) = f(f(1)) = f(1+1) = f(2) = 2/2 = 1$.

Paso inductivo fuerte (IF_1).— Supongamos que $\forall m \in \mathbb{Z}^+, m < k, \exists h \in \mathbb{Z}^+, f^{(h)}(n) = 1$, esto es, supongamos ciertas $P(1), P(2), \ldots, P(k-1)$. Dado k: si k es par, $f(k) = k/2$ y como $k/2 < k$, por la hipótesis de inducción, $P(k)$; si k es impar, $f(k) = k + 1$ es par y $f^{(2)}(k) = f(k+1) = \dfrac{k+1}{2}$, y como $1 < k$, $k + 1 < k + k = 2k$, esto es, $\dfrac{k+1}{2} < k$, de donde, por la hipótesis de inducción, $\exists h \in \mathbb{Z}^+, f^{(h)}(\dfrac{k+1}{2}) = 1$, por lo que $f^{(h+2)}(k) = 1$.

Conclusión ($\mathrm{IF}_0 \wedge \mathrm{IF}_1$).— Como se satisfacen el caso base y el paso inductivo fuerte, entonces del teorema 16.3 (pág. 810 de esta edición) de inducción fuerte se sigue lo buscado, a saber, que $\forall n \in \mathbb{Z}^+$ se satisface la afirmación $P(n)$. ■

Observación 16.1.1.— *Cfr. infra* conjetura de Collatz (pág. 1095 de esta edición).

Actividad 16.1

Demostremos que $\forall n \in \mathbb{Z}^+, 12 \mid (n^4 - n^2)$.

Vid. [122]: § 10.2 *Proofs by Strong Induction*, Proposición (pág. 188).

Actividad 16.2

Si x e y son dos palabras de $\{0,1\}^*$, entonces $x0y = y1x$.

§ 16.2 Inducción de Cauchy

Tanto en la inducción débil como en la fuerte, los pasos inductivos son «hacia adelante». En la inducción de Cauchy participan dos pasos inductivos, uno hacia adelante y otro hacia atrás.

Teorema 16.4 (Inducción de CAUCHY para $\mathbb{N}$)

Se satisface:

$$\begin{aligned} \mathrm{IC}_0 &\leftrightharpoons P(1); \\ \mathrm{IC}_1 &\leftrightharpoons (\forall k \in \mathbb{Z}^+)(P(k) \to P(2k)); \\ \mathrm{IC}_2 &\leftrightharpoons (\forall k \in \mathbb{Z}^+)(P(k) \to P(k-1)); \\ \mathrm{IC}_0 \wedge \mathrm{IC}_1 \wedge \mathrm{IC}_2 &\vdash \forall n \in \mathbb{Z}^+, P(n). \end{aligned}$$

Demostración.— Veamos que se satisfacen las hipótesis de la inducción débil para $\mathbb{N} \setminus \{0\}$. En efecto, por un lado, IC_0 es ID_0, por otro, por IC_1, de $P(k)$ se sigue $P(2k)$, y de ésta, por IC_2, se sigue $P(2k-1)$, de ésta, igualmente por IC_2, se sigue $P(2k-2)$, y así sucesivamente, hasta $P(k+1)$ (ya que $k+1 \leq 2k$). ■

Observación 16.2.0.— De IC_0 y IC_1 se sigue $\forall n \in \mathbb{N}, P(2^n)$.

Observación 16.2.1.— En realidad, pudiésemos usar cualquier función $f(k)$ en vez de $2k$ en IC_1, siempre que $(\forall k \in \mathbb{Z}^+)(f(k) > k)$, quedando el paso inductivo hacia adelante (IC_1) así: $(\forall k \in \mathbb{Z}^+)(P(k) \to P(f(k)))$.

Ejemplo 420

Demostremos que para números reales positivos, la media geométrica es menor o igual que la media aritmética, esto es, que $\forall x_1, x_2, \ldots, x_n \in \mathbb{R}^+$ $(\forall n \in \mathbb{Z}^+)$,

$$\sqrt[n]{x_1 x_2 \ldots x_n} \leq \frac{x_1 + x_2 + \ldots + x_n}{n}.$$

Resolución.— Siendo $P(n) \leftrightharpoons$«$(\forall x_1, x_2, \ldots, x_n \in \mathbb{R}^+) \left(\sqrt[n]{x_1 x_2 \ldots x_n} \leq \dfrac{x_1 + x_2 + \ldots + x_n}{n} \right)$», lo que nos proponemos es demostrar que $\forall n \in \mathbb{Z}^+, P(n)$. Para ello, apliquemos el teorema 16.4 (pág. 814 de esta edición) de inducción de CAUCHY:

Caso base (IC_0).— $P(1)$ es $\sqrt[1]{x_1} \leq \dfrac{x_1}{1}$, esto es, $x_1 \leq x_1$. Si bien fuese bastante con esto, demostremos también $P(2)$, ya que nos será de utilidad: $\sqrt[2]{x_1 x_2} \leq \dfrac{x_1 + x_2}{2}$ si, y sólo si, $4x_1x_2 \leq (x_1 + x_2)^2$ si, y sólo si, $0 \leq (x_1 - x_2)^2$. Observemos que acabamos de demostrar que dados dos números reales positivos cualesquiera, digamos r y s, se satisface $\sqrt[2]{r \cdot s} \leq \dfrac{r+s}{2}$. Este resultado es el que utilizaremos.

Paso inductivo hacia adelante (IC_1).— La hipótesis inductiva, $P(k)$, es $\sqrt[k]{x_1 x_2 \ldots x_k} \leq \dfrac{x_1 + x_2 + \ldots + x_k}{k}$, y la tesis inductiva, $P(2k)$ es $\sqrt[2k]{x_1 x_2 \ldots x_{2k}} \leq \dfrac{x_1 + x_2 + \ldots + x_{2k}}{2k}$; justamente por el resultado para dos números, siendo r y s, respectivamente, $\sqrt[k]{x_1 x_2 \ldots x_k}$ y

$\sqrt[k]{x_{k+1}x_{k+2}\ldots x_{2k}}$, tenemos que

$$\sqrt{\sqrt[k]{x_1x_2\ldots x_k}\cdot\sqrt[k]{x_{k+1}x_{k+2}\ldots x_{2k}}}\leq\frac{\sqrt[k]{x_1x_2\ldots x_k}+\sqrt[k]{x_{k+1}x_{k+2}\ldots x_{2k}}}{2};$$

por otra parte, de la hipótesis inductiva, tenemos que

$$\frac{\sqrt[k]{x_1x_2\ldots x_k}+\sqrt[k]{x_{k+1}x_{k+2}\ldots x_{2k}}}{2}\leq\frac{\frac{x_1+x_2+\ldots+x_k}{k}+\frac{x_{k+1}+x_{k+2}+\ldots+x_{2k}}{k}}{2};$$

como $\sqrt{\sqrt[k]{x_1x_2\ldots x_k}\cdot\sqrt[k]{x_{k+1}x_{k+2}\ldots x_{2k}}}=\sqrt[2k]{x_1x_2\ldots x_{2k}}$ y $\dfrac{\frac{x_1+x_2+\ldots+x_k}{k}+\frac{x_{k+1}+x_{k+2}+\ldots+x_{2k}}{k}}{2}=\dfrac{x_1+x_2+\ldots+x_{2k}}{2k}$, la última desigualdad queda

$$\sqrt[2k]{x_1x_2\ldots x_{2k}}=\frac{x_1+x_2+\ldots+x_{2k}}{2k},$$

esto es, precisamente la tesis inductiva $P(2k)$.

Paso inductivo hacia atrás (IC_2).— La hipótesis inductiva, $P(k)$, es $\sqrt[k]{x_1x_2\ldots x_k}\leq\dfrac{x_1+x_2+\ldots+x_k}{k}$; sea $x_k=\dfrac{x_1+x_2+\ldots+x_{k-1}}{k-1}$; como $\dfrac{x_1+x_2+\ldots+\frac{x_1+x_2+\ldots+x_{k-1}}{k-1}}{k}=\dfrac{x_1+x_2+\ldots+x_{k-1}}{k-1}$, tenemos que $\sqrt[k]{x_1x_2\ldots x_{k-1}\frac{x_1+x_2+\ldots+x_{k-1}}{k-1}}\leq\dfrac{x_1+x_2+\ldots+x_{k-1}}{k-1}$; de aquí,

$$x_1x_2\ldots x_{k-1}\frac{x_1+x_2+\ldots+x_{k-1}}{k-1}\leq\left(\frac{x_1+x_2+\ldots+x_{k-1}}{k-1}\right)^k,$$

de donde, $x_1x_2\ldots x_{k-1}\leq\left(\dfrac{x_1+x_2+\ldots+x_{k-1}}{k-1}\right)^{k-1}$, esto es, $\sqrt[k-1]{x_1x_2\ldots x_{k-1}}\leq\dfrac{x_1+x_2+\ldots+x_{k-1}}{k-1}$, es decir, $P(k-1)$, la tesis inductiva.

Conclusión ($IC_0\wedge IC_1\wedge IC_2$).— Como se satisfacen el caso base y ambos pasos inductivos, entonces del teorema 16.4 (pág. 814 de esta edición) de inducción de Cauchy se sigue lo buscado, a saber, que $\forall n\in\mathbb{Z}^+$ se satisface la afirmación $P(n)$. ■

Ejemplo 421

Demostremos por inducción de Cauchy que si sólo se dispone de sellos de 3 céntimos y de 5 céntimos, es posible formar cualquier franqueo de 8 o más céntimos.

[Cubit 62].

Resolución.— Demostremos, por inducción de Cauchy, que $\forall n\in\mathbb{N}\setminus\{0,1,\ldots,7\}$, $P(n)$, donde $P(n)$ es la afirmación «puede formarse un franqueo de n céntimos sólo con sellos de 3 y de 5 céntimos».

Para ello, apliquemos el teorema 16.4 (pág. 814 de esta edición) de inducción de Cauchy:

Caso base (IC_0).— El paso base de la inducción de Cauchy es común con la inducción débil y con la fuerte y ya lo analizamos en el ejemplo 415 (pág. 808 de esta edición).

Paso inductivo hacia adelante (IC_1).— $\forall k \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}$, se satisface que si $P(k)$, esto es, si $\exists m, n \in \mathbb{N}$ tales que $k = 3m + 5n$, entonces se satisface $P(2k)$, esto es, que $\exists m', n' \in \mathbb{N}$ tales que $2k = 3m' + 5n'$ (en efecto: $m' = 2m$, $n' = 2n$); en definitiva, dado un franqueo de $k \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}$ cts., basta con añadir la misma cantidad de sellos de 3 cts. y de 5 cts. que éste tuviese para formar un franqueo de $2k$ cts.

Paso inductivo hacia atrás (IC_2).— $\forall k > 8$, se satisface que si $P(k)$, esto es, si $\exists m, n \in \mathbb{N}$ tales que $k = 3m+5n$, entonces se satisface $P(k-1)$, esto es, que $\exists m', n' \in \mathbb{N}$ tales que $k-1 = 3m'+5n'$; veamos porqué:

- si el franqueo contuviese al menos dos sellos de 5 cts., sustituiríamos estos dos por tres de 3 cts. (es decir, $m' = m + 3$ y $n' = n - 2$);
- si el franqueo no contuviese al menos dos sellos de 5 cts. —esto es, si no contuviese ninguno o sólo contuviese uno—, como $k > 8$, debe contener al menos dos sellos de 3 cts. —pues de contener como mucho uno, el valor de k sería como mucho 8—, por lo que sustituiríamos dos sellos de 3 cts. por un sello de 5 cts. (es decir, $m' = m - 2$ y $n' = n + 1$).

Conclusión ($\mathrm{IC}_0 \wedge \mathrm{IC}_1 \wedge \mathrm{IC}_2$).— Como se satisfacen el caso base y ambos pasos inductivos, entonces del teorema 16.4 (pág. 814 de esta edición) de inducción de Cauchy se sigue lo buscado, a saber, que $\forall n \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}$ se satisface la afirmación $P(n)$. ■

§ 16.3 Inducción en un conjunto bien ordenado

Realmente, los métodos de demostración por inducción son válidos para cualquier conjunto numerable S que esté bien ordenado, con un primer elemento n_0 y la localización del siguiente elemento se base en la existencia de una función siguiente o sucesor $s(k)$ (recordemos la considerada por Peano).

Teorema 16.5 (Inducción débil para un conjunto bien ordenado)
Se satisface:

$$\frac{P(n_0) \qquad (\forall k \geq n_0)(P(k) \to P(s(k)))}{\forall n \in S, P(n)}.$$

Teorema 16.6 (Inducción fuerte para un conjunto bien ordenado)
Se satisface:
$$\frac{P(n_\circ) \qquad (\forall k \geq n_\circ)(P(n_\circ) \wedge \ldots \wedge P(k) \to P(s(k)))}{\forall n \in S, P(n)}$$

Teorema 16.7 (Inducción de CAUCHY para un conjunto bien ordenado)
Se satisface:
$$\frac{P(n_\circ) \qquad (\forall k \geq n_\circ)(P(k) \to P(s(s(k)))) \qquad (\forall k \geq n_\circ)(P(s(k)) \to P(k))}{\forall n \in S, P(n)}.$$

Ejemplo 422

¿Cómo procederíamos si quisiésemos demostrar por inducción una propiedad para todos los pares positivos?

Resolución.— Pudiésemos utilizar, bien la función siguiente doblemente aplicada como en la inducción de CAUCHY, bien una función siguiente alternativa: si S es el conjunto de los pares positivos, el primer elemento $n_\circ = 2$ y la función siguiente es $s(k) = k + 2$; es decir, $s(2) = 2 + 2 = 4$, $s(4) = 4 + 2 = 6$, y así sucesivamente. ■

§ 16.4 Inducción estructural

§ 16.4.0 Conjunto inductivo

Sean $A \neq \emptyset$, $B \subseteq A$, $B \neq \emptyset$ y

$$K = \{f_i^n : A^n \longrightarrow A \text{ tal que } \langle i, n\rangle \in I \times J\}\ ,$$

con $I, J \neq \emptyset$, $J \subseteq \mathbb{Z}^+$, no siendo necesariamente todas las f de K de la misma aridad.

Definición 16.0.— Decimos que $Y \subseteq A$ es inductivo sobre B para —o respecto de— K si, y sólo si,

- $B \subset Y$, y
- $\forall f \in K, \forall \mu \in Y^n, f(\mu) \in Y$ (Y es cerrado para K).

Llamamos al conjunto B, la *base* y a K el conjunto de *constructores*.

Ejemplo 423

Demostremos que $\mathbb{N}$ es inductivo sobre $B = \{0\}$ para $K = \{sig\}$ donde $sig : \mathbb{N} \longrightarrow \mathbb{N}$ (aridad 1) está definida por $sig(n) = n + 1$.

Resolución.— En efecto, $B = \{0\} \subset Y = \mathbb{N}$ y $\forall n \in \mathbb{N}$, $sig(n) = n + 1$. ■

Ejemplo 424

Sea el alfabeto $\sum = \{$ si, entonces, si no, fsi, mientras, hacer, fmientras, ;, ., $\leftarrow$, (,), suc, pred, x, t, $0, 1, 2, \ldots, 9, <, >, = \}$. Un *programa mientras* es cualquier hilera finita de símbolos de $\sum$ que satisface un conjunto determinado de reglas sintácticas. El conjunto de todos los programas mientras, PM, es inductivo sobre ASIG para K, donde

- ASIG $= \{x \leftarrow t$ tal que $x \in$ Vars $\wedge$ $t \in$ Terms$\}$, y
- $K = \{$;, si entonces si no fsi, mientras hacer fmientras $\}$.

y «;» denota concatenación.

Actividad 16.3

Demostremos el ejemplo anterior (no es difícil demostrar que todos los constructores producen programas mientras).

§ 16.4.1 Clausura o cierre inductivo de B para K

Definición 16.1.— Designada por B^+, la *clausura inductiva* (o, sinónimamente, *cierre inductivo*) de B para K es la intersección de todos los conjuntos inductivos sobre B para K; en realidad, el menor de todos ellos.

Una *definición constructiva* es $B^+ = \bigcup_{n\in\mathbb{N}} B_n$, estando la sucesión creciente $\{B_n\}_{n\in\mathbb{N}}$ definida por

$$B_0 = B,$$
$$B_{i+1} = B_i \cup \{f(\mu) : f \in K \wedge \mu \in B_i^n\}.$$

Ejemplo 425

$\mathbb{N}$ es clausura inductiva de $B = \{0\}$ para $K = \{sig\}$.

Resolución.—

$$\begin{aligned} B_0 &= \{0\}, \\ B_1 &= \{0\} \cup \{sig(0)\} = \{0, sig(0)\}, \\ B_2 &= \{0, sig(0)\} \cup \{sig(0), sig(sig(0))\} = \{0, sig(0), sig(sig(0))\}, \\ &\vdots \\ B^+ = \{0\}^+ &= \{0, sig(0), sig(sig(0)), sig(sig(sig(0))), \ldots\} \\ &= \mathbb{N} \end{aligned}$$

■

§ 16.4.2 Clausura libremente generada

Definición 16.2.— Decimos que la clausura inductiva, B^+, es libremente generada si, y sólo si, se satisface:

0. todo constructor genera elementos distintos, a partir de elementos distintos. O sea, todo constructor, $f : A^n \longrightarrow A$, es inyectivo (en realidad, su restricción $f : (B^+)^n \longrightarrow B^+$);
1. constructores distintos generan elementos distintos, es decir, $\forall f : A^m \longrightarrow A, \forall g : A^n \longrightarrow A$, $f((B^+)^m) \cap g((B^+)^n) = \emptyset$;
2. ningún constructor genera elementos del conjunto base, esto es, $\forall f \in K, \forall \mu \in (B^+)^n, f(\mu) \in B^+ \setminus B$.

De manera equivalente (y más abreviada), B^+ es libremente generada si, y sólo si,

$$(\forall x \in B^+)((x \in B) \veebar (\exists! f \in K, \exists! \mu \in (B^+)^n, x = f(\mu))).$$

Ejemplo 426

$\mathbb{N}$ es una clausura inductiva libremente generada.

Resolución.— En efecto, $\forall n \in \{0\}^+ = \mathbb{N}$, o bien $n \in \{0\}$ o bien $\exists! f = sig \in K, \exists! \mu = n - 1 \in (\{0\}^+)^1 = \mathbb{N}, n = sig(\mu)$. ■

Actividad 16.4

Demostremos que PM, esto es, ASIG$^+$ (*cfr. supra* ejemplo 424 [pág. 818 de esta edición]) es libremente generada.

§ 16.4.3 Principio de inducción estructural

Teorema 16.8 (Principio de inducción estructural)
Sea B^+ la clausura inductiva de B respecto de K y P una propiedad relativa a B^+, entonces:

$$\frac{[\text{IE}_0 \leftrightharpoons]\ \forall b \in B, Pb \qquad [\text{IE}_1 \leftrightharpoons]\ \forall f \in K, \forall \mu \in (B^+)^n, P\mu \to Pf(\mu)}{\forall x \in B^+, Px}$$

donde $P\mu \equiv Px_0 \wedge Px_1 \wedge \cdots \wedge Px_{n-1}$, siendo n la aridad de f.

Ejemplo 427

Demostremos por inducción estructural que si sólo se dispone de sellos de 3 céntimos y de 5 céntimos, es posible formar cualquier franqueo de 8 o más céntimos.

[Cubit 59].

Resolución.— Siendo la base y el conjunto de constructores (en este caso, sólo uno), $B = \{8, 9, 10\}$ y $K = \{sig^3\}$, respectivamente —donde $(\forall n \in \mathbb{N})(sig^3(n) = sig(sig(sig(n))))$, constructor de aridad 1—, la clausura inductiva B^+ de B para K viene dada por:

$$\begin{aligned}
B_0 &= \{8, 9, 10\}, \\
B_1 &= B_0 \cup \{f(\mu) : f \in K \wedge \mu \in B_0\} = B_0 \cup \{sig(8), sig(9), sig(10)\} = \{8, 9, 10, 11, 12, 13\}, \\
B_2 &= B_0 \cup \{f(\mu) : f \in K \wedge \mu \in B_1\} = B_1 \cup \{sig(8), sig(9), sig(10), sig(11), sig(12), sig(13)\} \\
&= \{8, 9, 10, 11, 12, 13, 14, 15, 16\}, \\
&\vdots \\
B^+ &= \bigcup_{n \in \mathbb{N}} B_n = \{8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, \ldots\} = \mathbb{N} \setminus \{0, 1, \ldots, 7\}
\end{aligned}$$

Demostremos, por inducción estructural, que $\forall n \in B^+$, $P(n)$, donde $P(n)$ es la afirmación «puede formarse un franqueo de n céntimos sólo con sellos de 3 y de 5 céntimos».

Para ello, apliquemos el teorema 16.8 (pág. 820 de esta edición) de inducción estructural:

Caso base (IE_0).— El paso base de la inducción estructural es común con la inducción débil, con la fuerte y con la de Cauchy y ya lo analizamos en el ejemplo 415 (pág. 808 de esta edición).

Paso inductivo estructural (IE_1).— $\forall \mu \in B^+$, se satisface que si $P\mu$, esto es, si $\exists m, n \in \mathbb{N}$ tales que $\mu = 3m + 5n$, entonces se satisface $P(sig^3(\mu))$, esto es, $P(\mu + 3)$, o sea, que $\exists m', n' \in \mathbb{N}$ tales que $\mu + 3 = 3m' + 5n'$ (en efecto: $m' = m + 3$, $n' = n$); en definitiva, si $\mu \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}$, basta con añadir un sello de 3 cts. para franquear $\mu + 3$.

Conclusión ($IE_0 \wedge IE_1$).— Como se satisfacen el caso base y el paso inductivo estructural, entonces del teorema 16.3 (pág. 810 de esta edición) de inducción estructural se sigue lo buscado, a saber, que $\forall n \in \mathbb{N} \setminus \{0, 1, \ldots, 7\}$ se satisface la afirmación $P(n)$. ■

Ejemplo 428 Verificación de la terminación de un segmento de programa

Demostremos que el siguiente segmento de programa termina. Utilicemos para ello la inducción estructural.

mientras $n > A$ **hacer**
  dec(n,2);
fin

Resolución.— En primer lugar, hablemos sobre la verificación de la terminación de un segmento de programa, en realidad, un segmento iterativo. Así, sin saber más sobre un segmento de programa, no tenemos datos suficientes para conocer la base, por lo que la igualamos a la entrada, $B = \{n_0\}$. Para cada entrada n_0 se define la clausura inductiva, $B^+(n_0)$. En principio, habrá, por tanto, tantas bases y clausuras inductivas como el dominio que imponga la restricción sobre los tipos de datos n y A, es decir, si éstos son naturales, pues un número numerable de ellos. No obstante, observemos que la demostración que hacemos es independiente de la entrada.

En este ejemplo, identificamos el constructor $f(n) = n - 2$, y la clausura inductiva $B^+(n_0) = \{n_0, f(n_0) = n_0 - 2, f^2(n_0) = n_0 - 4, \ldots\}$. Demostremos, por inducción estructural, que $\forall n \in B^+(n_0)$, Pn, donde mediante el predicado monádico P:

$$Pn \leftrightharpoons \exists k \in \mathbb{N}, f^k(n) \leq A,$$

expresamos la terminación del bucle mientras.

Para el único elemento de la base, n_0, es claro que existe un $k \in \mathbb{N}$ tal que $f^k(n_0) \leq A$ y, por tanto, el segmento de programa termina (si $n_0 \leq A$, entonces, $k = 0$ y si $n_0 = A + p$, entonces, $k = \lceil p/2 \rceil$). Sea $m \in \mathbb{Z}^+$; supongamos que se satisface para $n_0 - 2m$ y demostremos que también es cierto para $f(n_0 - 2m) = n_0 - 2(m+1)$. En efecto, si para $n_0 - 2m$ existe un $k \in \mathbb{N}$ tal que $f^k(n_0 - 2m) \leq A$, entonces, para $n_0 - 2(m+1)$ basta coger $k' = k - 1$, siempre que $k \geq 1$, es decir, cuando $n_0 > A$.

Ni qué decir tiene que en este proceso es posible sustituir los predicados de terminación por predicados de verificación de la corrección parcial, o incluso reforzar los de terminación, de manera que solucionemos el problema de la corrección total. ■

§ 16.5 Inducción bien fundada (noetheriana)

§ 16.5.0 Conjunto bien fundado

Sea un conjunto no vacío C y una relación diádica $\prec$, definida en él. Si $\prec$ es un orden parcial estricto en C, decimos que C es un *conjunto bien fundado* (c.b.f.) para $\prec$, si no contiene sucesiones decrecientes infinitas.

Observación 16.5.0.— Por si hubiera lugar a confusión, debemos comentar que existen varias diferencias entre conjuntos bien fundados y *conjuntos bien ordenados*. Recordemos que decimos que un orden $\preceq$, es bueno para un conjunto C, precisamente si todo subconjunto de C tiene primer elemento para el orden $\preceq$. Para empezar, la relación $\preceq$ es de orden (reflexiva, antisimétrica y transitiva), obligada, por ejemplo, a ser reflexiva, para tener así sentido la definición de buen orden con conjuntos unitarios, y por ejemplo, a ser total, para que tengan mínimo todos los conjuntos de dos elementos. Es decir, que todo orden bueno es total. *Si un conjunto está bien ordenado por* $\preceq$, *entonces está bien fundado por su orden irreflexivo asociado*, $\prec$. Pero el recíproco, no es cierto: del carácter parcial de $\prec$ es imposible deducir el carácter total de $\preceq$.

Ejemplo 429 Algunos modelos y contramodelos de conjuntos bien fundados

Los siguientes conjuntos parcialmente ordenados son conjuntos bien fundados.

0. $(\mathbb{N}; <)$, siendo $<$ el orden parcial estricto habitual;
1. $(\Sigma^*; \prec_{\text{long}})$;

Los siguientes conjuntos parcialmente ordenados no son conjuntos bien fundados.

0. $(\mathbb{Z}; <)$, siendo $<$ el orden parcial estricto habitual, pues, por ejemplo, la sucesión $-2n$ $(n \in \mathbb{N})$ es estrictamente decreciente e infinita;
1. $(\{1/n : n \in \mathbb{N}\}; <)$, siendo $<$ el orden parcial estricto habitual en los racionales, pues precisamente el mismo conjunto es una sucesión estrictamente decreciente e infinita.

§ 16.5.1 Inducción de un orden bien fundado

Teorema 16.9 (Orden bien fundado inducido)
Sean $(D_2, \prec_2)$ un conjunto bien fundado y $f : D_1 \longrightarrow D_2$ una aplicación. Definamos:

$$\forall a, b \in D_1, a \prec_1 b :\equiv f(a) \prec_2 f(b) \tag{16.0}$$

entonces, D_1 es un conjunto bien fundado con respecto a $\prec_1$.

Observación 16.5.1.— Debido a este teorema, podremos definir $\mathbb{N} \times \mathbb{N}$ como conjunto bien fundado para ciertos órdenes parciales estrictos; algunos ejemplos son:

0. $(m', n') \prec_1 (m, n) :\equiv m' < m$;
1. $(m', n') \prec_2 (m, n) :\equiv m' + n' < m + n$;
2. $(m', n') \prec_{\text{lex}} (m, n) :\equiv (m' < m) \vee (m' = m \wedge n' < n)$ (lexicográfico).

Ejemplo 430

Verifiquemos la terminación del segmento de programa del ejemplo 428 (pág. 821 de esta edición) utilizando órdenes bien fundados.

Resolución.— Para verificar la terminación de una iteración (segmento S), utilizamos el teorema 16.9 para inducir un orden bien fundado en el dominio de la iteración, D_S (producto cartesiano de los dominios de sus variables). Llamamos función terminadora (o, sinónimamente, *función limitadora*) a esa $t : D_S \longrightarrow \mathbb{N}^n$. Debemos demostrar que $t(D_S) \subseteq \mathbb{N}^n$ y que el valor en cada iteración es cada vez menor, según $\prec_S$, esto es, que $\forall \mu \in D_S$, $\sigma(\mu) \prec_S \mu$, lo que equivale, por definición de $\prec_S$, a que $\forall \mu \in D_S$, $t(\sigma(\mu)) \prec_S t(\mu)$.

Si P es una precondición del bucle, lo anterior queda, en el caso particular de $n = 1$, $\forall \mu \in D_S$,

$$P\mu \to t(\mu) \geq 0,$$
$$P\mu \to t(\sigma(\mu)) < t(\mu).$$

Para el segmento de programa del ejemplo 428 (pág. 821 de esta edición), observamos que es posible elegir como función terminadora $t(n) = n - A$. El resultado de una iteración, $\sigma(n) = n - 2$. La precondición del bucle viene dada por su guarda, $Pn \equiv n > A$, que implica, por un lado, que $n - A \geq 0$ y, por otro, que $t(\sigma(n)) = t(n-2) = (n-2) - A < t(n) = n - A$. ∎

Sea C un conjunto bien fundado respecto de $\prec$. Decimos que $m \in C$ es un *elemento minimal* en C respecto de $\prec$ precisamente si no tiene predecesores según $\prec$, esto es, si, y sólo si, no existe ningún elemento x de C, tal que $x \prec m$. Cuando el elemento minimal es único, lo llamamos *elemento mínimo*.

§ 16.5.2 Principio de inducción bien fundada

Teorema 16.10 (Inducción en un conjunto bien fundado)
Sea C un conjunto bien fundado respecto de $\prec$ y P un predicado monádico con argumento un elemento de C. Se satisface que todo elemento minimal en C satisface P y si dado cualquier elemento no minimal x de C es cierto que todos los elementos anteriores a él satisfacen P, entonces x también satisface P; esto es,

$$\frac{(\forall x \in C)((x \text{ es minimal } \to P(x)) \land (x \text{ no es minimal } \to ((\forall y \in C)(y < x \to P(y)) \to P(x)))}{\forall x \in C, P(x)}$$

También se le conoce como *principio de inducción noetheriana* (de Emmy Noether) o *principio de inducción completa/extensa en conjuntos bien fundados*.

Ejemplo 431

Demostremos que todas las palabras tienen longitud no negativa.

Resolución.— La relación «ser subpalabra estricta de» es de orden parcial estricto en el conjunto de todas las palabras de un alfabeto, siendo además este conjunto bien fundado respecto de dicho orden por ser la palabra vacía el elemento mínimo de este conjunto respecto a dicha relación.

Definimos la longitud de una palabra como el número de letras que tiene. La longitud de una subpalabra y de otra x es menor o igual que la de esta última.

Existe un elemento minimal, a saber, la palabra vacía, que tiene longitud 0, esto es, una longitud no negativa.

Dada una palabra no vacía, suponiendo que todas sus subpalabras tienen longitud no negativa, por la propiedad anterior la palabra tiene también longitud no negativa.

Por tanto, por inducción bien fundada, todas las palabras tienen longitud no negativa. ■

Ejemplo 432

Verifiquemos la terminación del segmento de programa del ejemplo 428 (pág. 821 de esta edición) utilizando inducción bien fundada.

Resolución.— Consideremos el conjunto $C = \{A+1, A+2, A+3, A+4, \dots\}$ y el orden parcial estricto habitual en los naturales, $<$. Sea P el predicado de terminación definido por $Px \equiv \exists k \in \mathbb{N}, x - 2k \leq A$. Vemos que claramente es cierto, de hecho ni siquiera hace falta inducción, pues dado x, basta elegir $k \geq \lceil (x - A)/2 \rceil$.

El caso base de la inducción bien fundada consiste en verificar la validez de $P(A+1)$, lo que es trivial, pues $k=1$. El paso inductivo, también es trivial, pues si para todo $y < x, \exists k_y \in \mathbb{N}, y - 2k_y \leq A$, entonces, para $x = y + 1$, basta coger $k_x = \text{máx}\{k_y : y < x\} + 2$.

Claro que también podíamos haber razonado como anteriormente y coger un conjunto bien fundado para cada entrada, $C(n_0) = \{n_0, n_0 - 2, n_0 - 4, \ldots\}$. No obstante aquí el razonamiento es más peregrino, pues hemos de localizar un elemento minimal, que claramente sabemos que será $A+1$ o $A+2$, dependiendo de los valores de n_0 y de A; eso, siempre que el orden sea el habitual. ■

§ 16.6 Propuesta de más actividades

Actividad 16.5

Demostremos por inducción la suma parcial enésima de la progresión aritmética de primer término 1, esto es, que $\forall n \in \mathbb{N}, 1 + 2 + \cdots + n = \dfrac{n \cdot (n+1)}{2}$.

Con miras a su resolución.— Como complemento a la demostración algebraica que debiese hacer quien lee, veamos un programita:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
# definiendo las variables
var('k,n')

# definiendo la suma de 1 a n
def sum1a(n):
        return sum(i for i in range(1, n + 1));

# definiendo la fórmula para la suma de 1 a n
def form_sum1a(n):
        return n * (n + 1) / 2

# definiendo el predicado
def P(n):
        return sum1a(n) == form_sum1a(n)

# demostrando el caso base P(1)
if P(1):
        print("Se satisface el caso base.")
elif not P(1):
        print("No se satisface el caso base.")
else:
        print("No sé cómo he llegado hasta aquí.")
```



```
# demostrando el paso inductivo: k*(k+1)/2 + (k+1) == (k+1)*(k+2)/2,
# esto es, si form_sum1a(k) + (k+1) es igual a form_sum1a(k+1)
is_equal = simplify((form_sum1a(k) + (k+1)) - form_sum1a(k+1))
if is_equal == 0:
print("Se satisface el paso inductivo.")
elif is_equal != 0:
print("No se satisface el paso inductivo.")
else:
print("No sé cómo he llegado hasta aquí.")
```

Actividad 16.6

Demostremos por inducción que $\forall n \in \mathbb{N}, 6 | (n^3 + 5n)$.

Actividad 16.7

Demostremos por inducción que $\forall n \in \mathbb{Z}, 1^2 + 2^2 + \ldots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Actividad 16.8

Una demostración clásica, de que todos los números enteros positivos son iguales, o sea, que sólo hay un número entero positivo, es la siguiente: Sea $A(n) \leftrightharpoons$ «en cualquier conjunto de n números enteros positivos, todos ellos son iguales». Demostremos, por inducción débil, que, $\forall n \in \mathbb{Z}^+, A(n)$. Si $n = 1$, $A(1) \equiv$ «en cualquier conjunto unitario de números naturales, todos son iguales», es, evidentemente, cierto. Suponemos cierto $A(k)$ y demostramos $A(k+1)$: notemos por P cualquier conjunto de $k+1$ números naturales; quitemos uno de ellos, por ejemplo, p_0; en el conjunto $P \setminus \{p_0\}$, al contener k números, todos ellos son iguales (por hipótesis de inducción); pongamos de nuevo a p_0 en el conjunto y quitemos otro número distinto, digamos p_1; en el conjunto $P \setminus \{p_1\}$, al contener k números, todos ellos son iguales (lo que implica que p_0 es igual a todos los de $P \setminus \{p_0\}$). De este modo, hemos demostrado que $A(k) \to A(k+1)$. Así que por inducción débil, es cierto, que, $\forall n \in \mathbb{Z}^+, A(n)$. ¿O no?

La propuesta de la siguiente actividad es similar a la de la anterior.

Actividad 16.9

Algunas personas afirman que en cualquier conjunto finito de bolas de colores, todas ellas tienen el mismo color. Dicen que lo han demostrado. Pero en realidad es una mala utilización de la inducción débil. A continuación, su «demostración». ¿Somos capaces de encontrar el error?

Sea $P(n)$ la afirmación «En cualquier conjunto de bolas de colores, todas ellas tienen el mismo color». $P(1)$ es evidente, pues con una sola bola, todas ellas tienen

el mismo color. Supongamos ahora $P(k)$ (la hipótesis inductiva), esto es, que en cualquier conjunto de k bolas, todas tienen el mismo color. Sea A un conjunto de $k+1$ bolas. Quitemos una de las bolas del conjunto, digamos, a_1. Por la hipótesis de inducción, todas las bolas de $A \setminus \{a_1\}$ tienen el mismo color. Ahora devolvamos a_1 a A y quitemos una bola distinta, digamos, a_2. Las bolas restantes en A, todas tienen el mismo color, de nuevo por la hipótesis inductiva. Aún más, ya ha sido demostrado que a_2 tiene el mismo color que las k bolas de $A\setminus\{a_2\}$. Por tanto, todas las $k+1$ bolas tienen el mismo color. Así hemos establecido que $P(k) \to P(k+1)$. Hemos demostrado que se satisfacen el paso base y el paso inductivo. Finalmente, aplicando el principio de inducción débil, se sigue que en cualquier cojunto finito de bolas de colores, no importa lo grande que sea, todas las bolas tienen el mismo color.

[SEL 4:13]. *Cfr.* Bradley [190]: § 3.7 *Mathematical Induction*, ejemplo 5 (págs. 132–134).
Cfr. qq. [151]: § 3.3 Inducción matemática, problema 51 (págs. 237–238).

Una vez descubierto el error de la demostración en las actividades anteriores, podremos pensar en diferentes versiones de la misma; la siguiente actividad es un ejemplo de ello.

Actividad 16.10

Definamos el máximo entre $x, y \in \mathbb{N}$, como $\text{máx}(x, y) = x$ (si $x \geq y$) y $\text{máx}(x, y) = y$ (si $x < y$). Consideremos el predicado $A(n) \leftrightharpoons (\forall x)(\forall y)(\text{si } \text{máx}(x, y) = n, \text{entonces } x = y)$. Veamos: $A(0)$ es trivialmente cierto. Supongamos que se satisface $A(k)$ y demostremos $A(k+1)$; sea $\text{máx}(x, y) = k+1$ y sean $x_ = x - 1$, e $y_ = y - 1$, por lo que $\text{máx}(x_, y_) = k$ y por hipótesis inductiva, $x_ = y_$, de donde $x = x_ + 1 = y_ + 1 = y$. Por tanto, por inducción débil, es cierto, que, $\forall n \in \mathbb{N}, A(n)$.

Actividad 16.11

Utilicemos inducción para demostrar que $n^3 - n$ es divisible por 3 siempre que n sea un entero positivo.

Observación.— Observemos que éste es el enunciado con $p = 3$ del Teorema Pequeño de Fermat —*cfr. infra* teorema 18.95 (pág. 1021 de esta edición)—.

[SEL 4:16]. *Cfr.* Rosen [151]: § 3.3 Inducción matemática, ejemplo 3 (pág. 225).

Actividad 16.12

Utilicemos inducción débil para demostrar que $7^{n+2} + 8^{2n+1}$ es divisible por 57 para todo $n \in \mathbb{N}$.

[SEL 4:17]. *Cfr.* Rosen [152]: § 5.1 *Mathematical Induction*, ejemplo 9 (pág. 322).

Actividad 16.13

Recordemos que es posible definir el conjunto de fórmulas bien construidas formadas con variables proposicionales (fórmulas bien formadas), operadores lógicos del conjunto $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ y los valores V y F. Demostremos por inducción estructural que en toda fórmula bien construida, hay el mismo número de paréntesis izquierdos que derechos.

[SEL 4:19]. *Cfr.* Rosen [151]: § 3.4 Definiciones recursivas e inducción estructural, ejemplos 13 (pág. 249) y 10 (pág. 245).

Actividad 16.14

Sea un montón de n piedras que subdividimos en n montones de una sola piedra cada uno, dividiendo sucesivamente cada montón de piedras en dos más pequeños. Cada vez que dividimos un montón, anotamos el producto de los números de piedras en cada uno de los dos nuevos montones. Por ejemplo, tras dividir un montón en dos, digamos, uno con r piedras y el otro con s piedras, anotamos el producto $r \cdot s$. Demostremos, a ser posible por inducción fuerte, que independientemente de cómo dividamos los montones, la suma de los productos anotados es $n(n-1)/2$.

Cfr. Rosen [151]: problema 40 (pág. 237).

Actividad 16.15

Ahora, en vez de calcular el producto $r \cdot s$, calculemos $(r \cdot s) \cdot (r + s)$. De manera similar a la actividad anterior, sumemos todos estos productos al final del proceso. Demostremos, a ser posible por inducción fuerte, que la suma de los productos es $n(n^2 - 1)/3$.

Cfr. Hopkins [191] (págs. 7–10).

Actividad 16.16

Utilicemos la inducción estructural para demostrar que $h(T)$, el número de hojas de un árbol binario completo T, es uno más que $i(T)$, el número de vértices internos de T.

Cfr. Rosen [151]: problema 44 (pág. 254).

Actividad 16.17

Imaginemos una isla donde 100 personas, todas poseedoras de una lógica perfecta, son encarceladas por un dictador loco. No hay escape, salvo una regla extraña. Cualquier persona prisionera puede acercarse a los guardias por la noche y pedirle salir. Si tienen ojos verdes, serán liberadas. Si no, las lanzarán al volcán. Casualmente, las 100 personas prisioneras tienen ojos verdes, pero han vivido allí desde que nacieron, y el dictador se ha asegurado de que no sepan el color de sus ojos. No hay superficies reflectantes, toda el agua está en recipientes opacos, y, más importante, no se les permite comunicarse entre ellas. Aunque se ven durante el recuento de cada mañana. Sin embargo, todas estas personas saben que ninguna se arriesgaría a salir sin estar absolutamente segura del éxito. Tras mucha presión por parte de diversos grupos de derechos humanos, el dictador acepta a regañadientes que visitemos la isla y hablemos con las personas prisioneras con las siguientes condiciones: sólo se puede hacer una declaración, y no nos está permitido darles nueva información.

¿Qué pudiésemos decir para ayudar a liberar a las personas prisioneras sin desatar la ira del dictador? Después de mucho pensarlo les decimos: «Por lo menos una persona entre ustedes tiene los ojos verdes». El dictador sospecha pero se calma al pensar que esta declaración no ha cambiado nada. Nos vamos y la vida en la isla parece continuar como antes. Pero 100 mañanas más tarde, no queda ninguna persona prisionera, ya que todas pidieron salir la noche anterior. ¿Cómo superamos en ingenio al dictador?

Observación.— Es posible ver un vídeo sobre esta cuestión (el audio está en inglés pero los subtítulos están disponibles en 24 idiomas, incluyendo español e inglés): https://www.youtube.com/watch?v=98TQv5IAtY8. La solución: mín. 1:53, justo cuando se ve un signo de interrogación blanco y grande con un fondo rojo. La solución se basa en conocimiento común (https://en.wikipedia.org/wiki/Common_knowledge_(logic)) e inducción. En TED(Ed), encontramos una lección (en inglés) sobre esta cuestión: https://ed.ted.com/lessons/the-famously-difficult-green-eyed-logic-puzzle-alex-gendler.

[SEL 4:20].

Actividad 16.18

Supongamos una reunión a la que asisten n personas en la que todas se saludan entre sí una, y sólo una, vez. Demostremos por inducción que el número de personas que ha saludado un número impar de veces es par.

Observación.— Encontraremos más adelante más cuestiones sobre saludos —*cfr. v. gr. infra* ejemplo 612 (pág. 1137 de esta edición)—.

§ 16.7 Bibliografía

[122] Richard HAMMACK. *Book of proof*. Hammack, Richmond, Virginia, EE. UU., 3.ª ed., 2022.

[147] Herbert Bruce ENDERTON. *Elements of Set Theory*. Academic Press, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1977.

[151] Kenneth Howard ROSEN. *Matemática discreta y sus aplicaciones*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 5.ª ed., 2004. (La 5.ª edición es la última en español).

[152] Kenneth Howard ROSEN. *Discrete Mathematics and its Applications*. McGraw-Hill, Nueva York, Nueva York (US-NY), Estados Unidos de América, 7.ª ed., 2012.

[190] James BRADLEY. *Introduction to discrete mathematics*. Addison-Wesley, Reading, Middlesex, Mancomunidad de Massachusetts (US-MA), Estados Unidos de América, 1988.

Sección C

Álgebra abstracta

Capítulo 17

Lógica de estructuras

¿Puede alguien pensar que porque seamos ingenieros, no nos preocupa la belleza o que no intentamos construir estructuras bellas, sólidas y permanentes? ¿No están las genuinas funciones de fuerza siempre en coordinación con condiciones no escritas de armonía? [...] Además, existe una atracción, un particular encanto en lo colosal al que las teorías ordinarias del arte no se aplican.

(Alexandre Gustave Eiffel, 1832–1923.
En: Henry Petroski, *Remaking the World: Adventures in Engineering*, 1998, pág. 173).

Como decíamos al presentar la lógica de clases, la caracterización del modo de estar relacionadas las entidades de una colección, su organización interna a partir de los comportamientos —determinados por funciones— entre sus entidades, está en la esencia de la lógica de estructuras.

§ 17.0 Estructura algebraica

Definición 17.0.— Decimos que un conjunto $A \neq \emptyset$ posee una *estructura algebraica*, precisamente si sobre él se define un número finito de leyes de composición, internas o externas. Solemos decir que A es el conjunto *soporte* (o, sinónimamente, *portador*) de la estructura.

Observación 17.0.0.— Pudiésemos comparar una estructura algebraica con el esqueleto humano, considerándolo como el armazón elemental de nuestros cuerpos. Si en este momento nos comparamos, apreciaremos grandes diferencias entre las personas, pero si nos pudiésemos comparar dentro de 10,000 años, a primera vista nos veríamos prácticamente iguales. Aunque la apariencia externa sea diferente, la estructura interna es la misma. De igual forma, las estructuras matemáticas representan esta semejanza subyacente en situaciones que aparentemente son distintas. La utilidad de la formalización de las estructuras radica en la generalización resultante; a partir de tal formalización, se deducen unas propiedades, características comunes a todos los ejemplos de la misma estructura, que servirán para demostrar otros hechos (consecuencias). Estos nuevos hechos, se verificarán en cualquier caso particular de esa misma estructura. Si en el ejemplo del esqueleto decimos «la tibia y el peroné están unidos», no necesitaríamos confirmar de nuevo esto en todas las personas, pues todas tienen la misma estructura. La idea es que una estructura matemática es una abstracción de propiedades comunes encontradas en diversas situaciones.

§ 17.1 Magma

Definición 17.1.— Sean un conjunto $A \neq \emptyset$ y $* : A \times A \longrightarrow A$ una operación diádica en A. En tal caso, decimos que el par $(A; *)$ es un *magma* (o, sinónimamente, *grupoide*).

Definición 17.2.— Sean $(A; *)$ un magma y $a \in A$. Decimos que a tiene *potencia enésima* en $(A; *)$ precisamente si $(\exists x \in A)(x = a * \overset{n}{\smile\!\!\cdots} * a)$. Decimos entonces que x es la potencia enésima de a en $(A; *)$ y escribimos $x = a^n$.

Definición 17.3.— Sean $(A;*)$ un magma y $a \in A$. Decimos que a tiene *raíz enésima* en A precisamente si $(\exists x \in A)(a = x * \overset{n}{\overbrace{\cdots}} * x)$. Decimos entonces que x es una raíz enésima de a en $(A;*)$ y escribimos $x = a^{\frac{1}{n}}$ (o, sinónimamente, $x = \sqrt[n]{a}$).

Ejemplo 433

Sea la operación $x * y = (x \cdot y)$ mód 11, en el conjunto $\{0, 1, 2, \ldots, 10\}$. ¿Cuáles son las potencias de 2? ¿Y las raíces de 2?

Resolución.— Se satisface:

- las potencias de 2 son: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^9 = 6$, $2^{10} = 1$, $2^{11} = 2, \ldots$, esto es, la secuencia 1, 2, 4, 8, 5, 10, 9, 7, 3, 6, repetida una y otra vez;
- las raíces de 2 son: $\sqrt[1]{2} = 2$, $\nexists\sqrt[2]{2}$, $\sqrt[3]{2} = 7$, $\nexists\sqrt[4]{2}$, $\nexists\sqrt[5]{2}$, $\nexists\sqrt[6]{2}$, $\sqrt[7]{2} = 8$, $\nexists\sqrt[8]{2}$, $\nexists\sqrt[9]{2} = 6$, $\nexists\sqrt[10]{2}$, $\sqrt[11]{2} = 2, \ldots$, en definitiva, $\sqrt[1+10n]{2} = 2$, $\sqrt[3+10n]{2} = 7$, $\sqrt[7+10n]{2} = 8$, $\sqrt[9+10n]{2} = 6$ con $n \in \mathbb{N}$; el resto no existen. ■

Ejemplo 434

Sea $\mathbb{N}$ y la suma habitual. ¿Cuáles son las potencias de 2? ¿Y las raíces de 2?

Resolución.— Se satisface:

- las potencias de 2 son: $2^1 = 2$, $2^2 = 4$, $2^3 = 6$, $2^4 = 8$, $2^5 = 10$, $2^6 = 12$, $2^7 = 14$, $2^8 = 16$, $2^9 = 18$, $2^{10} = 20$, $2^{11} = 22, \ldots$, esto es, $2^n = 2 \cdot n$, siendo $\cdot$ el producto habitual entre naturales;
- las raíces de 2 son: $\sqrt[1]{2} = 2$, $\sqrt[2]{2} = 1$, $\nexists\sqrt[n]{2}$ para $n \in \mathbb{N}_{>2}$. ■

§ 17.1.0 Elementos idempotentes y singulares

Definición 17.4.— Sean $(A;*)$ un magma y $a \in A$. Decimos que a es *idempotente* en A para $*$, precisamente si $a * a = a$.

Definición 17.5.— Sean $(A;*)$ un magma. Decimos que $*$ es *idempotente* en A, precisamente si $(\forall a \in A)\,(a * a = a)$.

Definición 17.6.— Sean $(A;*)$ un magma y $s \in A$. Decimos que s es:

a. *singular* (o, sinónimamente, *absorbente*) *por la izquierda* en A para $*$, precisamente si $(\forall a \in A)\,(s * a = s)$;

b. *singular* (o, sinónimamente, *absorbente*) *por la derecha* en A para $*$, precisamente si $(\forall a \in A)\,(a * s = s)$;

c. *singular* (o, sinónimamente, *absorbente*) en A para $*$, precisamente si lo es por la izquierda y por la derecha.

Ejemplo 435 (Algunos modelos de magmas)

0. Consideremos la interpretación $(\mathbb{N}; \cdot)$, con $\cdot$ el producto habitual numérico:
   - constituye un modelo de magma;
   - existen dos elementos idempotentes: 0 y 1;
   - sólo existe un elemento absorbente: 0.
1. Las interpretaciones $(\mathbb{N}; +)$, $(\mathbb{Z}; +)$, $(\mathbb{Z}; -)$, $(\mathbb{Z}; \cdot)$, $(\mathbb{Q}; +)$, $(\mathbb{Q}; -)$, $(\mathbb{Q}; \cdot)$, $(\mathbb{Q} \setminus \{0\}; /)$, $(\mathbb{R}; +)$, $(\mathbb{R}; -)$, $(\mathbb{R}; \cdot)$, $(\mathbb{R} \setminus \{0\}; /)$, $(\mathbb{C}; +)$, $(\mathbb{C}; -)$, $(\mathbb{C}; \cdot)$ y $(\mathbb{C} \setminus \{\langle 0, 0\rangle\}; /)$ son (modelos de) magmas.
2. El par $(\mathbb{N}; -)$ no es un (modelo de) magma, ya que $-$ no es una operación en $\mathbb{N}$. Tampoco son (modelos de) magma ni $(\mathbb{N}; /)$ ni $(\mathbb{Z}; /)$ ni $(\mathbb{Q}; /)$ ni $(\mathbb{R}; /)$ ni $(\mathbb{C}; /)$.
3. Cualquiera de los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, con la operación diádica máximo, $a * b = \text{máx}(a, b)$, es un (modelo de) magma.
4. La interpretación $(\{33, 77, 99\}, *)$, estando $*$ definida, $\forall a, b \in \{33, 77, 99\}$, por $a * b = \text{mcd}(a, b)$, no es un (modelo de) magma.
5. El par $(\mathbb{R}^n; \cdot)$ con $\cdot$ el producto escalar, no es un modelo de magma (el producto escalar de vectores no es un vector).

§ 17.1.1 Homomorfismo

Definición 17.7.— Dados dos magmas $(X; *)$ e $(Y; \circ)$, decimos que una aplicación $f : X \longrightarrow Y$ es un *homomorfismo* (o, sinónimamente, *morfismo*), precisamente si $\forall x, y \in X$, $f(x * y) = f(x) \circ f(y)$.

Definición 17.8.— Dados dos magmas $(X; *)$ e $(Y; \circ)$, decimos que un homomorfismo $f : X \longrightarrow Y$ es:

a. un *monomorfismo*, precisamente si f es inyectiva;

b. un *epimorfismo*, precisamente si f es sobreyectiva;

c. un *isomorfismo*, precisamente si f es biyectiva;

d. un *endomorfismo*, precisamente si $X = Y$ y $* \equiv \circ$;

e. un *automorfismo*, precisamente si f es endomorfismo e isomorfismo.

Teorema 17.0

La composición de homomorfismos es un homomorfismo.

Teorema 17.1

Dados dos magmas $(X;*)$ e $(Y;\circ)$ y $f: X \longrightarrow Y$ un homomorfismo, se satisface que $f(X)$, esto es, $\{y \in Y : \exists x \in X, f(x) = y\}$, es *parte estable* de $(Y;\circ)$.

Definición 17.9.— Llamamos *imagen homomorfa* de $(X;*)$ a la estructura algebraica $(f(X);\circ)$.

§ 17.2 Semigrupo (magma asociativo)

Definición 17.10.— Sea $(X;*)$ un magma. Decimos que $*$ es *asociativa* en X, precisamente si $\forall x, y, z \in X$,

$$(x * y) * z = x * (y * z),$$

en cuyo caso decimos que $(X;*)$ es un *magma asociativo*.

Definición 17.11.— Decimos que $(X;*)$ es un *semigrupo*, precisamente si es un magma asociativo.

Ejemplo 436 (Algunos modelos de semigrupos)

0. Las siguientes interpretaciones constituyen (modelos de) semigrupos: $(\mathbb{N};+)$, $(\mathbb{N};\cdot)$, $(\mathbb{Z};+)$, $(\mathbb{Z};\cdot)$, $(\mathbb{Q};+)$, $(\mathbb{Q};\cdot)$, $(\mathbb{R};+)$, $(\mathbb{R};\cdot)$,$(\mathbb{C};+)$ y $(\mathbb{C};\cdot)$.

1. Los (modelos de) magmas $(\mathbb{Z};-)$, $(\mathbb{Q};-)$, $(\mathbb{R};-)$ no son (modelos de) semigrupos, pues $-$ no es asociativa en esos conjuntos (por ejemplo, $-4 = (1-2)-3 \neq 1-(2-3) = 2$). Tampoco son (modelos de) semigrupos los (modelos de) magmas $(\mathbb{Q}\setminus\{0\};/)$ y $(\mathbb{R}\setminus\{0\};/)$.

2. Cualquiera de los conjuntos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, con la operación diádica máximo, $a * b = \text{máx}(a,b)$, es un (modelo de) semigrupo.

3. Sea $A = \{0,1,2\}$ y la operación

$*$	0	1	2
0	1	2	0
1	2	0	1
2	0	1	2

entonces $(A; *)$ es un (modelo de) semigrupo abeliano.

4. El par $(\mathbb{R}^n; \times)$ con $\times$ el producto vectorial, no es un modelo de semigrupo ya que el producto vectorial no es asociativo (de paso, notemos que tampoco es conmutativo).

Observación 17.2.0.— En referencia a demostrar la asociativa, pudiésemos tener en cuenta la *prueba de asociatividad de* LIGHT[0] y la *prueba de asociatividad de* ABDALI para operaciones conmutativas[1].

Ejemplo 437

Sea $(C; +)$ un semigrupo en el que se satisface $(\forall x, y \in C)(x + y = y + x \to x = y)$. Demostremos que todo $c \in C$ es idempotente, esto es, que $c + c = c$.

[EFO 3.6.2019:2b].

Resolución.— Que $(C; +)$ sea un semigrupo significa que la ley de composición $+$ es una operación asociativa en C, esto es, se satisface, $\forall c \in C$:

$$\begin{aligned} c + c &\in C, && (+\text{ operación}) \\ c + (c + c) &= (c + c) + c. && (+\text{ asociativa}) \end{aligned} \tag{17.0}$$

Tomando (17.0) (siendo $x = c$ e $y = c + c$) como el antecedente de la implicación que según el enunciado satisfacen los elementos de C, se tiene la igualdad buscada, a saber, $c = c + c$. ■

Ejemplo 438

Sea $(C; +)$ un semigrupo abeliano. Sea R la relación diádica definida en C por $(\forall x, y \in C)\ (xRy \leftrightarrow x + y = y)$.

0. Estudiemos si R satisface las propiedades reflexiva, simétrica, antisimétrica, transitiva y conexa y digamos qué tipo de relación es y por qué;
1. Proporcionemos un ejemplo de conjunto C y considerando R actuando en él, mostremos cuáles son las clases de equivalencia, las clases de tolerancia (vecindades) o dibujemos un diagrama de HASSE, dependiendo de que R sea una relación de equivalencia, una relación de tolerancia o una relación de orden en C.

[EPF 14.5.2019:2a].

Resolución.— Veamos.

[0] *Vid. v. gr.* https://en.wikipedia.org/wiki/Light%27s_associativity_test.
[1] *Vid.* https://www.jstor.org/stable/3613856.

0. Dados cualesquiera elementos x e y de C,

   I. R no tiene por qué ser reflexiva, pues es posible proporcionar un contraejemplo: si $(C; +)$ es el semigrupo abeliano $(\mathbb{Z}^+; +)$, entonces ningún elemento x satisface $x + x = x$, por lo que en realidad, R no sólo no es reflexiva en $\mathbb{Z}^+$, sino que es irreflexiva;

   II. R tampoco tiene por qué ser simétrica, por ejemplo, consideremos el monoide abeliano aditivo de los naturales, $(\mathbb{N}; +)$, se tiene que $0R1$ pues $0 + 1 = 0$ pero $1\neg R0$ ya que $1 + 0 = 0 \neq 1$;

   III. R sí es antisimétrica; en efecto, sean cuales sean $a, b \in C$, se tiene que $aRb \leftrightarrow a+b = b$ y también que $bRa \leftrightarrow b + a = a$, por lo que, como $+$ es conmutativa en C, se sigue que $a = b$;

   IV. R también es transitiva; así es, para cualesquiera $a, b, c \in C$:

$$aRb \leftrightarrow a + b = b, \tag{17.1}$$

$$bRc \leftrightarrow b + c = c. \tag{17.2}$$

   de donde:

$$\begin{aligned} a + c &= a + (b + c) && \text{(por (17.2))} \\ &= (a + b) + c && \text{(+ es asociativa)} \\ &= b + c && \text{(por (17.1))} \\ &= c, && \text{(por (17.2))} \end{aligned}$$

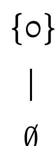
   esto es, aRc;

   V. sin embargo, R no es conexa (fuertemente completa), ya que, por ejemplo, en el semigrupo abeliano $(\mathbb{Z}^+; +)$, $1 + 2 = 3 \neq 2$ y $2 + 1 = 3 \neq 1$ por lo que ni 1 está relacionado con 2 ni 2 está relacionado con 1.

   Observemos que R no es una relación de orden parcial estricto, pues no es irreflexiva para ciertos semigrupos abelianos $(C; +)$ —aunque sí lo es en $(\mathbb{Z}^+; +)$, no lo es, por ejemplo, en $(\mathbb{N}; +)$ con $+$ la suma habitual entre naturales, pues $0R0$—. Se trata, pues, de una relación diádica antisimétrica y transitiva y no necesariamente reflexiva ni irreflexiva (hasta donde yo sé no existe una denominación estándar para ellas).

1. Si bien hemos demostrado que R no tiene por qué ser reflexiva mediante la provisión de un contraejemplo, es posible aportar un ejemplo de que sí puede serlo y por tanto que puede ser un orden: la relación de inclusión, $\subseteq$, en el conjunto potencia de un conjunto, es una relación de orden total. En efecto, consideremos un conjunto A, $C = 2^A$ y $+$ la unión de conjuntos. Entonces, la relación del ejemplo queda definida por $(\forall X, Y \in 2^A)(XRY \leftrightarrow X \cup Y = Y)$, y en definitiva por $(\forall X, Y \in 2^A)(XRY \leftrightarrow X \subseteq Y)$. Es decir, en el conjunto potencia de un conjunto, R

coincide con la relación de inclusión. Pensemos entonces, por ejemplo, en que A sea un conjunto unitario, digamos $A = \{0\}$, entonces $C = \{\emptyset, \{0\}\}$ y su diagrama de Hasse es:



Recordemos, no obstante, que para poder construir el diagrama de Hasse de una relación basta que ésta sea antisimétrica y transitiva (por ejemplo, la relación $\subset$ de inclusión estricta de conjuntos). ■

Teorema 17.2
Si $(X;*)$ es un semigrupo, entonces, el centro de X es parte estable de $(X;*)$.

§ 17.3 Magmas no necesariamente asociativos

Destacamos tres: magma alternativo, magma asociativo para la potencia y magma flexible.

§ 17.3.0 Magma alternativo

Una propiedad menos fuerte (exige menos) que la asociatividad es la alternatividad.

Definición 17.12 (Alternatividad).— Sea $(X;*)$ un magma. Decimos que:

- $*$ es *alternativa por la izquierda* en $X \risingdotseq (\forall x, y \in X)\,((x*x)*y = x*(x*y))$;
- $*$ es *alternativa por la derecha* en $X \risingdotseq (\forall x \in X)\,(y*(x*x) = (y*x)*x)$;
- $*$ es *alternativa* en $X \risingdotseq *$ es alternativa por la izquierda y por la derecha en X.

Teorema 17.3
Todo semigrupo, es decir, todo magma asociativo, es un magma alternativo.

El recíproco no es cierto. Por ejemplo, el álgebra de los *octoniones*[2] es alternativo pero no asociativo (ni conmutativo).

[2] *Vid. v. gr.* https://en.wikipedia.org/wiki/Octonion.

§ 17.3.1 Magma asociativo para la potencia

Definición 17.13 (Asociatividad para la potencia).— Sea $(X; *)$ un magma. Decimos que es un *magma asociativo para la potencia* precisamente si $(\forall x \in X)\,((x * x) * x = x * (x * x))$.

Teorema 17.4
Todo magma en el que todos sus elementos son idempotentes es un magma asociativo para la potencia.

Teorema 17.5
Todo magma asociativo es un magma asociativo para la potencia.

El recíproco no es cierto. Por ejemplo, el álgebra de los *sedeniones*[3] y el álgebra de los *trigintaduoniones*[4] son asociativos para la potencia pero no asociativos (ni conmutativos). Ninguno de ellos es alternativo.

§ 17.3.2 Magma flexible

Definición 17.14 (Flexibilidad).— Sea $(X; *)$ un magma. Decimos que es un *magma flexible* precisamente si $(\forall x, y \in X)\,((x * y) * x = x * (y * x))$.

Teorema 17.6
Todo magma asociativo, todo magma conmutativo, todo magma alternativo, todos ellos, son magmas flexibles.

Las álgebras de los octoniones, de los sedeniones y de los trigintaduoniones son flexibles.

§ 17.4 Monoide

Definición 17.15.— Sean $(X; *)$ un magma y $e \in X$. Decimos que:

- e es el *elemento neutro* (o, sinónimamente, *unidad* o *identidad*) *por la izquierda* en X para $*$ si, y sólo si, $(\forall x \in X)\,(e * x = x)$;
- e es el *elemento neutro* (o, sinónimamente, *unidad* o *identidad*) *por la derecha* en X para $*$ si, y sólo si, $(\forall x \in X)\,(x * e = x)$;
- e es el *elemento neutro* (o, sinónimamente, *unidad* o *identidad*) en X para $*$ si, y sólo si, lo es por la izquierda y por la derecha.

[3] *Vid. v. gr.* https://en.wikipedia.org/wiki/Sedenion.
[4] *Vid. v. gr.* https://en.wikipedia.org/wiki/Trigintaduonion.

Llamamos *elementos no triviales de* X a los elementos de X distintos del neutro.

Definición 17.16.— Decimos que $(X;*)$ es un *monoide*, precisamente si es un semigrupo con identidad.

Observación 17.4.0.— Llamamos *semigrupo unitario* a un semigrupo con identidad. Análogamente, llamamos *magma unitario* a un magma con identidad. Un semigrupo con identidad es un magma asociativo y unitario.

Teorema 17.7

Sean $(A;*)$ un monoide y $e \in A$ el elemento neutro para $*$. Se satisface que:

0. e es único: $(\forall e' \in A)((\forall a \in A)(e' * a = a * e' = a) \to e = e')$;
1. e es idempotente: $e * e = e$.

Ejemplo 439

Sea C un conjunto y $*$ una operación en C. Supongamos que existe elemento neutro para $*$ en C y que, cualesquiera $x, y, z \in C$ satisfacen $x * (y * z) = (x * z) * y$. Demostremos que $(C;*)$ es una estructura abeliana.

[EPF 14.5.2019:2b].

Resolución.— Sea $e \in C$ el elemento neutro de $*$ en C. Veamos que $*$ es una operación conmutativa en C. En efecto, $\forall x, y \in C$, se tiene que:

$$\begin{aligned} x * y &= e * (x * y) && \text{(por ser } e \text{ el elemento neutro de } * \text{ en } X) \\ &= (e * y) * x && \text{(porque } * \text{ satisface: } \forall x, y, z \in X, x * (y * z) = (x * z) * y) \\ &= y * x. && \text{(por ser } e \text{ el elemento neutro de } * \text{ en } X) \end{aligned}$$

■

Ejemplo 440

Sea $*$ una operación en un conjunto X en el que existe elemento neutro para $*$ y satisface para todo $x, y, z \in X$, $x * (y * z) = (x * z) * y$.

a. $*$ es conmutativa y asociativa en X.
b. $*$ es conmutativa en X, pero no asociativa.
c. $*$ no es conmutativa en X, aunque sí asociativa.
d. $*$ ni es conmutativa ni asociativa en X.

[TT], [EFE 3.7.2024:6] (tipo test).

Resolución.— Del ejemplo anterior sabemos que $*$ es conmutativa en X. Demostremos ahora que $*$ es asociativa en X:

$$\begin{aligned} x*(y*z) &= x*(z*y) && \text{(porque $*$ es conmutativa en X)} \\ &= (x*y)*z. && \text{(porque $*$ satisface: $\forall x,y,z \in X, x*(y*z)=(x*z)*y$)} \end{aligned}$$

Solución.— Opción a. ■

Ejemplo 441

Sea $*$ una operación en un conjunto X en el que existe elemento neutro para $*$ y satisface para todo $x, y, z \in X$, $x*(y*z) = (x*y)*z$, ¿cuál de las siguientes afirmaciones es verdadera?

a. $*$ es conmutativa y asociativa en X.
b. $*$ es conmutativa en X, pero no asociativa.
c. $*$ es asociativa en X y puede que conmutativa.
d. $*$ ni es conmutativa ni asociativa en X.

[TT], [EFE 29.1.2025:6] (tipo test).

Resolución.— Según el enunciado, $*$ es asociativa en X. Analicemos las opciones.

a. No es verdadera; un contraejemplo es la operación diádica producto de matrices cuadradas, que es asociativa y tiene elemento neutro (la matriz identidad), pero no es conmutativa.

b. No es verdadera, pues sí que es asociativa, por el enunciado.

c. Es verdadera; sí es asociativa por el enunciado y pudiese ser conmutativa —en el primer apartado mencionamos un ejemplo de operación asociativa y no conmutativa, mientras que un ejemplo de operación asociativa y conmutativa es $+$ en $\mathbb{N}$—.

d. No es verdadera, pues sí que es asociativa, por el enunciado.

Solución.— Opción c. ■

Ejemplo 442

Sea $(C;+)$ un monoide abeliano en el que el único elemento invertible es el neutro. Sea R la relación diádica definida en C por

$$xRy \leftrightarrow (\exists c \in C)(x + c = y),$$

siendo x e y elementos de C.

0. Estudiemos si R satisface o las propiedades: I, reflexiva; II, simétrica; III, antisimétrica; IV, transitiva, y V, conexa (fuertemente completa) y VI, ¿qué tipo de relación es? y VII, ¿por qué?
1. Proporcionemos un ejemplo de monoide abeliano $(C;+)$ en el que el único elemento simetrizable es el neutro y considerando R actuando en él, hallemos las clases de tolerancia y las clases maximales de tolerancia, las clases de equivalencia o dibujemos un diagrama de Hasse, dependiendo de que R sea una relación de tolerancia, una relación de equivalencia o una ordenación en $(C;+)$.

[EFO 3.6.2019:2a], [EFE 22.6.2022:3].

Resolución.—

0. Dados cualesquiera elementos x e y de C y notando por 0 el elemento neutro de $+$ en C, que existe, ya que $(C;+)$ es un monoide:

   I. R sí es reflexiva, pues para todo $x \in C$,

   $$x + 0 = x;$$

   II. R no tiene por qué ser simétrica, por ejemplo, consideremos el monoide abeliano aditivo de los naturales, $(\mathbb{N};+)$, se tiene que $1R3$ pues $1+2 = 3$ pero $3\neg R1$ ya que $(\neg\exists c \in \mathbb{N})(3+c = 1)$ —en realidad, la hipótesis de que el único elemento invertible en $(C;+)$ es el neutro de $+$ implica esto—;

   III. R sí es antisimétrica; en efecto, sean cuales sean $a, b \in C$, de

   $$aRb \leftrightarrow (\exists c_1 \in C)(a + c_1 = b) \tag{17.3}$$

   y

   $$bRa \leftrightarrow (\exists c_2 \in C)(b + c_2 = a) \tag{17.4}$$

   se tiene que

   $$\begin{aligned} b &= a + c_1 && \text{(por (17.3))} \\ &= (b + c_2) + c_1, && \text{(por (17.4))} \end{aligned}$$

de donde por ser $+$ asociativa, tener elemento neutro y ser una operación (aplicación),

$$c_2 + c_1 = 0$$

y como el único elemento invertible es el 0, se tiene que

$$c_1 = c_2 = 0;$$

IV. R también es transitiva; así es, para cualesquiera $a, b, c \in C$:

$$aRb \leftrightarrow (\exists c_1 \in C)(a + c_1 = b), \tag{17.5}$$

$$bRc \leftrightarrow (\exists c_2 \in C)(b + c_2 = c), \tag{17.6}$$

de donde:

$$\begin{aligned} c &= b + c_2 && \text{(por (17.6))} \\ &= (a + c_1) + c_2 && \text{(por (17.5))} \\ &= a + (c_1 + c_2) && \text{(+ es asociativa)} \\ &= a + c_3, && \text{(+ es operación)} \end{aligned}$$

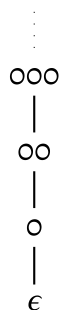
con $c_3 \in C$ (ya que $c_3 = c_1 + c_2$ y $+$ es operación en C), y por tanto, aRc;

V. sin embargo, R no es conexa (fuertemente completa), ya que, por ejemplo, el conjunto C de todas las palabras finitas de un alfabeto determinado Σ con la operación concatenación de palabras es un monoide abeliano (la palabra vacía ϵ es el neutro) —la notación más habitual para este monoide $(C; +)$ es Σ^* y se le conoce como *monoide libre sobre el alfabeto* Σ—; pensemos, por ejemplo, en $\Sigma = \{0, 1\}$, donde las palabras 0 y 1 no son comparables por R (no existe ninguna palabra que concatenada a 0 de la palabra 1 ni reciprocamente);

VI. se trata de una relación de orden parcial;

VII. R es una relación de orden parcial porque satisface las propiedades reflexiva, antisimétrica y transitiva (y no es total porque no satisface la conexa).

1. Sea, por ejemplo, $\Sigma = \{0\}$; la palabra vacía ϵ es el único elemento invertible de Σ^* (en otras palabras, la única forma de obtener ϵ por concatenación de dos palabras es $\epsilon + \epsilon = \epsilon$). El diagrama de HASSE de R, en este caso un orden total en Σ^*, puede dibujarse sólo parcialmente, por ser infinito numerable el número total de palabras:





Definición 17.17.— Sea $(X; *)$ un magma unitario, con identidad $e \in X$ y sea $x \in X$. Decimos que:

- x es *simetrizable por la izquierda* en X para $*$ si, y sólo si, $(\exists y \in X)\,(y * x = e)$, y llamamos a y el simétrico por la izquierda de x;
- x es *simetrizable por la derecha* en X para $*$ si, y sólo si, $(\exists y \in X)\,(x * y = e)$, y llamamos a a y el simétrico por la derecha de x);
- x es *simetrizable* (o, sinónimamente, *invertible* o *neutralizable*) en X para $*$ si, y sólo si, lo es a la vez por la izquierda y por la derecha. En este caso, si $(\exists y \in X)\,(x * y = y * x = e)$, decimos que y es el *elemento inverso* (o, sinónimamente, *elemento simétrico* o *elemento neutralizador*) de x.

Teorema 17.8

Si $(X; *)$ es un monoide, y un elemento $a \in X$ es simetrizable, esto es, tiene un simétrico por la izquierda y un simétrico por la derecha, entonces estos dos son iguales y, por lo tanto, a tiene simétrico; en otras palabras: en un monoide, ser simetrizable equivale a tener simétrico.

Teorema 17.9

Si $(X; *)$ es un monoide, entonces el simétrico de cualquier elemento simetrizable es único y el conjunto $\mathrm{Sim}\,(X; *) \subseteq X$, de todos los elementos simetrizables de X, es parte estable de $(X; *)$.

Teorema 17.10

En un monoide, si un elemento idempotente es simetrizable, entonces su simétrico también es idempotente.

Definición 17.18.— Sean $(X; *)$ un monoide y $z \in X$. Decimos que:

- z es *regular* (o, sinónimamente, *simplificable*) *por la izquierda* en X para $*$ si, y sólo si, $(\forall x, y \in X)\,(z * x = z * y \to x = y)$;
- z es *regular* (o, sinónimamente, *simplificable*) *por la derecha* en X para $*$ si, y sólo si, $(\forall x, y \in X)\,(x * z = y * z \to x = y)$;

- z es *regular* (o, sinónimamente, *simplificable*) en A para $*$ si, y sólo si, lo es por la izquierda y por la derecha.

Teorema 17.11
En un monoide se satisface que el elemento neutro es regular y que todo elemento simetrizable es regular.

Ejemplo 443 (Algunos modelos de monoides, y otros)

0. Los magmas $(\mathbb{Z}; -)$, $(\mathbb{Q}; -)$ y $(\mathbb{R}; -)$ tienen sólo identidad por la derecha.

1. $(\mathbb{N}; +)$, $(\mathbb{N}; \cdot)$, $(\mathbb{Z}; +)$, $(\mathbb{Z}; \cdot)$, $(\mathbb{Q}; +)$, $(\mathbb{Q}; \cdot)$, $(\mathbb{R}; +)$, $(\mathbb{R}; \cdot)$, $(\mathbb{C}; +)$ y $(\mathbb{C}; \cdot)$ son monoides conmutativos, cuyos elementos neutros son 0, 1, 0, 1, 0, 1, 0, 1, $(0, 0)$ y $(1, 0)$, respectivamente.

2. En $(\mathbb{N}; +)$, el único elemento simetrizable es 0. En $(\mathbb{N}; \cdot)$, el único elemento simetrizable es 1. En $(\mathbb{Z}; +)$, $(\mathbb{Q}; +)$, $(\mathbb{R}; +)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$, $(\mathbb{R} \setminus \{0\}; \cdot)$ y $(\mathbb{C} \setminus \{(0, 0)\}; \cdot)$, todos los elementos son simetrizables. En $(\mathbb{Z}; \cdot)$ los únicos elementos simetrizables son -1 y 1.

3. En $(\mathbb{N}; +)$, $(\mathbb{Z}; +)$, $(\mathbb{Q}; +)$, $(\mathbb{R}; +)$, $(\mathbb{N} \setminus \{0\}; \cdot)$, $(\mathbb{Z} \setminus \{0\}; \cdot)$, $(\mathbb{Q} \setminus \{0\}; \cdot)$ y $(\mathbb{R} \setminus \{0\}; \cdot)$, todo elemento es regular.

4. Dado un conjunto X, $(2^X; \cup)$ tiene estructura de monoide abeliano.

5. Sea $n \in \mathbb{N}$ y $M_0(n)$ el conjunto de los múltiplos no negativos de n, entonces $(M_0(n); +)$ tiene estructura de monoide abeliano; el elemento neutro es el 0.

6. $(\mathbb{N}; \mathrm{mcm})$ tiene estructura de monoide abeliano; el elemento neutro es el 1 que, además, es el único simetrizable.

7. Sean X un conjunto y 2^{X^2} el conjunto de todas las relaciones diádicas en X (también notado Rel_X) y sea $\circ$ la composición de relaciones, entonces $(2^{X^2}; \circ)$ tiene estructura de *monoide*, siendo I_X (relación de identidad en X) el elemento neutro y $\emptyset$ (la relación nula en X) un elemento absorbente (un cero).

Teorema 17.12
Si X es un conjunto, entonces $(X^X; \circ)$ es un *submonoide* del monoide $(2^{X^2}; \circ)$ de las relaciones diádicas.

Si X e Y son dos conjuntos, notamos el conjunto de todas las funciones de X a Y por Y^X, es decir, $Y^X = \{f : f \text{ es una función de } X \text{ a } Y\}$.

Definición 17.19.— En un monoide, es posible definir recursivamente la *potencia enésima de un elemento*:

$$x^0 = e,$$
$$x^{n+1} = x * x^n, \text{ si } n \in \mathbb{Z}^+.$$

Además, si x es simetrizable y $x\prime$ es su simétrico, es posible definir la *potencia enésima negativa de un elemento* x,

$$x^{-n} = (x\prime)^n, \text{ con } n \in \mathbb{Z}^+.$$

Observación 17.4.1.— Las estructuras unitarias que estamos estudiando en estos epígrafes, semigrupo, monoide y grupo, son clases de magma. Existen otras muchas (*cuasigrupo*, *bucle*, etc. —*cfr. v. gr.* https://en.wikipedia.org/wiki/Magma_(algebra)—), si bien su estudio particular queda restringido a ámbitos más específicos.

Ya han aparecido en nuestro estudio las estructuras de *magma asociativo* (semigrupo), *magma alternativo* y *magma unitario*. Por motivos de nuestra exposición, mencionamos en este punto sólo una más, a saber, *magma con inversos*.

Definición 17.20.— Decimos que un magma $(X; *)$ es un *magma con inversos* si, y sólo si, para todo elemento de X existe su simétrico para $*$ en X.

Teorema 17.13

Sean $(X; *)$ e $(Y; \circ)$ dos magmas unitarios y con inversos y $f : X \to Y$ un homomorfismo. Entonces, $\forall x \in X$ se satisface que:

0. si e es el neutro en $(X; *)$, entonces $f(e)$ es el neutro en $(Y; \circ)$;
1. si x' es el simétrico de x para $*$ en X, entonces $f(x')$ es el simétrico de $f(x)$ para $\circ$ en Y.

Observación 17.4.2.— No obstante lo dicho, veremos situaciones en que en el magma los elementos tendrán simétrico lateral o existirá un neutro lateral; cuestión de adaptar el nombre de la clase de magma según las circunstancias.

§ 17.5 Grupo

Definición 17.21.— Sea un conjunto $G \neq \emptyset$ y $*$ una ley de composición diádica definida en G. Decimos que la estructura $(G; *)$ es un *grupo* si, y sólo si, $*$ satisface:

0.º, $(\forall x, y \in G)\,(x * y \in G)$ ($*$ es l.c.i. en G);

1.º, $(\forall x, y, z \in G)\,((x * y) * z = x * (y * z))$ ($*$ es asociativa en G);

2.º, $(\exists e \in G)\,(\forall x \in G)\,(x * e = e * x = x)$ (existe el elemento neutro de $*$ en G);

3.º, $(\forall x \in G)\,(\exists y \in G)\,(x * y = y * x = e)$ (todo elemento de G tiene simétrico en G para $*$).

Teorema 17.14
Una estructura algebraica es un grupo si, y sólo si, dicha estructura es un monoide en el que todo elemento es simetrizable.

Teorema 17.15
El elemento neutro de un grupo es único.

Teorema 17.16
Todo elemento de un grupo tiene un único simétrico. Dicho único simétrico de x suele representarse por x'.

Observación 17.5.0.— Si la operación fuese *conmutativa*, esto es, si $\forall x, y \in G$, $x * y = y * x$, entonces diríamos de la estructura $(G; *)$ que es *conmutativa* (o, sinónimamente, *abeliana*). En este caso, es frecuente representar la operación por el símbolo $+$ (representación aditiva). En este caso, suele designarse el neutro por 0 y el simétrico de un elemento x por $-x$. El *simétrico aditivo* de un elemento suele denominarse su *opuesto*. Si la operación se representa por $\cdot$ (multiplicativamente), entonces el neutro se designa por 1 y el simétrico de un elemento x por x^{-1}. El *simétrico multiplicativo* de un elemento suele denominarse su *recíproco*.

Observación 17.5.1 (Axiomática del sistema formal de teoría de grupos).— Rayano con cuando estudiamos diversos sistemas axiomáticos para la teoría de conjuntos[5] y el sistema axiomático de la aritmética elemental[6], destacamos en esta observación el sistema formal de teoría de grupos. Con base la lógica de primer orden con identidad[7] y con signos primitivos G (el dominio de referencia no vacío), $*$ (la operación diádica), e(o, sinónimamente, 0 o 1) (el nombre del elemento neutro o unidad) y $'$ (la operación monádica, elemento simétrico), el *sistema formal de teoría de grupos* es, y sólo es, el que tiene por axiomas:

$(\forall x, y, z)((x * y) * z = x * (y * z))$ (ley asociativa),

[5] *Vid. supra* § 14 (p. 752).
[6] *Vid. supra* § 15.0.2 (p. 788).
[7] *Vid. supra* § 5.6.0 (pág. 423 de esta edición).

$(\forall x)(x * e = x)$ (ley de existencia del elemento neutro/unidad),
$(\forall x)(\exists x')(x * x' = e)$ (ley de existencia del elemento simétrico);

si además satisface

$(\forall x, y)(x * y = y * x)$ (ley conmutativa),

se trata del *sistema formal de teoría de grupos conmutativos*.[8]

Ejemplo 444 (Algunos modelos y contramodelos de grupos)

0. $(\mathbb{N}; +)$ no es grupo —0 es el único simetrizable—.
1. $(\mathbb{N}; \cdot)$ no es grupo —1 es el único simetrizable—.
2. $(\mathbb{Z}; +)$ es grupo conmutativo.
3. $(\mathbb{Z}; \cdot)$ no es grupo —1 es el único simetrizable)—.
4. $(\mathbb{Q}; +)$ y $(\mathbb{Q} \setminus \{0\}; \cdot)$ son grupos conmutativos.
5. $(\mathbb{Q}; \cdot)$ no es grupo —0 no es simetrizable—.
6. $(\mathbb{R}; +)$ y $(\mathbb{R} \setminus \{0\}; \cdot)$ son grupos conmutativos.
7. $(\mathbb{R}; \cdot)$ no es grupo —0 no es simetrizable—.
8. $(\mathbb{C}; +)$ y $(\mathbb{C} \setminus \{(0, 0)\}; \cdot)$ son grupos conmutativos.
9. $(\mathbb{C}; \cdot)$ no es grupo —$(0, 0)$ no es simetrizable—.

Ejemplo 445

Demostremos que un semigrupo $(S; *)$ con más de un elemento idempotente no puede ser un grupo.

[EFE 25.6.2019:2b1].

Resolución.— Reescribamos la afirmación como «Si $(S; *)$ es un semigrupo con más de un elemento idempotente, entonces $(S; *)$ no es un grupo», esto es, en la forma $P \to Q$. Razonemos por reducción al absurdo: supongamos $P \wedge \neg Q$, esto es, que existen dos elementos distintos a y b de S idempotentes —es decir, $a * a = a$ y $b * b = b$— y que $(S; *)$ es un grupo; entonces, por esto último,

[8] Por ejemplo, el grupo $SO(3)$ de rotaciones en tres dimensiones no es conmutativo —visualicemos, a modo de ejemplo, una esfera y su polo norte, que está en OY: rotemos primero respecto de OX, de OY a OZ, y después respecto de OY, de OZ a OX, quedando dicho polo en OX; rotemos ahora primero respecto de OY, de OZ a OX (el polo permanece en su sitio), y después respecto de OX, de OY a OZ, quedando dicho polo en OZ; he aquí pues un ejemplo de no conmutatividad—. En las páginas siguientes veremos más ejemplos de grupos no conmutativos y de grupos conmutativos.

existe el elemento neutro, digamos e, y los simétricos de a y b, digamos a' y b'; entonces:

$$\begin{aligned} a' * a &= a' * (a * a) && (a \text{ es idempotente}) \\ &= (a' * a) * a && ({}^* \text{ es asociativa}) \\ &= e * a && (\text{definición de simétrico}) \\ &= a, \end{aligned}$$

por lo que a sería un neutro por la derecha, aunque de forma similar pudiésemos demostrar que lo sería también por la izquierda y por tanto que $a = e$; igual ocurre con b:

$$\begin{aligned} b' * b &= b' * (b * b) && (b \text{ es idempotente}) \\ &= (b' * b) * b && ({}^* \text{ es asociativa}) \\ &= e * b && (\text{definición de simétrico}) \\ &= b; \end{aligned}$$

es decir, que $a = e$ y $b = e$ y, por lo tanto, $a = b$ (el elemento neutro de un grupo es único), en contra de nuestra hipótesis de partida de ser distintos; en otras palabras, hemos llegado a una fórmula insatisfactible partiendo de haber supuesto $P \wedge \neg Q$; aplicando reducción al absurdo concluimos lo que queríamos demostrar: $P \rightarrow Q$. ■

Ejemplo 446

Proporcionemos un ejemplo de un semigrupo $(S; \square)$ que no sea grupo. Razonemos el porqué.

[EFE 25.6.2019:2b2].

Resolución.— Según el ejemplo 445 (pág. 851 de esta edición), bastaría un semigrupo con más de un elemento idempotente, si bien un ejemplo más sencillo pudiese ser: $\Sigma^* = (C; +)$, siendo $\Sigma = \{0\}$ y $C = \{\epsilon, 0, 00, 000, \ldots\}$. Σ^* es semigrupo, ya que la operación concatenación de palabras es asociativa. Además, es monoide, siendo el elemento neutro la palabra vacía ϵ. Pero no es grupo porque no existe el simétrico de una palabra no vacía, esto es, si $a \neq \epsilon$, no existe una palabra a' tal que $a' + a = \epsilon$ (la única palabra que tiene simétrico es la vacía: $\epsilon + \epsilon = \epsilon$). ■

Ejemplo 447

Sea $\mathbb{Z}$ el conjunto de los enteros y sea k un entero. Sea la ley de composición diádica en $\mathbb{Z}$ definida por: $\forall x, y \in \mathbb{Z}, x *_k y = x + y + k$, donde $+$ es la suma habitual en $\mathbb{Z}$. ¿Es $(\mathbb{Z}; *_k)$ un grupo abeliano sea cual sea el entero k?

[AIC 10.4.2019:3]. *Cfr.* Anzola y Caruncho [140]: problema 10.15 (pág. 214).

Resolución.—

I. La ley de composición $*_k$ es una operación (una ley de composición interna) en $\mathbb{Z}$, pues la suma habitual lo es; por tanto, $(\mathbb{Z}; *_k)$ es un magma;

II. $\forall x, y \in \mathbb{Z}$, se tiene que

$$\begin{aligned} x *_k y &= x + y + k \\ &= y + x + k \\ &= y *_k x; \end{aligned}$$

así, de I y II se sigue que $(\mathbb{Z}; *_k)$ es un magma abeliano (conmutativo), sea cual sea $k \in \mathbb{Z}$;

III. $\forall x, y, z \in \mathbb{Z}$, se tiene —debido a la asociativa y conmutativa de $+$ en $\mathbb{Z}$— que

$$\begin{aligned} (x * y) *_k z &= (x + y + k) *_k z \\ &= (x + y + k) + z + k \\ &= x + y + z + k + k; \end{aligned}$$

por otro lado —debido igualmente a la asociativa y conmutativa de $+$ en $\mathbb{Z}$—, se tiene que

$$\begin{aligned} x * (y *_k z) &= x *_k (y + z + k) \\ &= x + (y + z + k) + k \\ &= x + y + z + k + k; \end{aligned}$$

como ambos resultados son iguales, se tiene que $*_k$ es asociativa en $\mathbb{Z}$;
así, de I, II y III se sigue que $(\mathbb{Z}; *_k)$ es un semigrupo abeliano, sea cual sea $k \in \mathbb{Z}$;

IV. el elemento neutro es $-k$; por ser una estructura abeliana basta demostrarlo por un lado; por ejemplo, veamos que $\forall x \in \mathbb{Z}, x *_k (-k) = x$; en efecto, por ser $(\mathbb{Z}; +)$ un grupo abeliano (en $\mathbb{Z}$, $+$ es asociativa y 0 es el elemento neutro para $+$):

$$\begin{aligned} x *_k (-k) &= x + (-k) + k \\ &= x + (-k + k) \\ &= x + 0 \\ &= x; \end{aligned}$$

así, de I, II, III y IV se sigue que $(\mathbb{Z}; *_k)$ es un monoide abeliano, sea cual sea $k \in \mathbb{Z}$;

V. similarmente, por ser una estructura conmutativa, para encontrar el elemento simétrico de uno dado, basta buscarlo por un lado; sea x' el simétrico de x, entonces, debe satisfacerse que $x *_k x' = -k$; por definición de $*_k$, esto significa que $x + x' + k = -k$, y de aquí, por ser $(\mathbb{Z}; +)$ un grupo abeliano, se tiene que: $x' = -x - 2k$; por tanto, existe el simétrico para cualquier $x \in \mathbb{Z}$; así, de I, II, III, IV y V se sigue que $(\mathbb{Z}; *_k)$ es un grupo abeliano, sea cual sea $k \in \mathbb{Z}$. ■

Ejemplo 448

Sea el conjunto $\{0, 2, 4\}$ y la operación $x +_6 y = (x + y)$ mód 6 donde $+$ es la suma habitual entre enteros y a mód b es el resto de la división de a por b. Demostremos que $(\{0, 2, 4\}; +_6)$ tiene estructura de grupo abeliano.

[EFO 17.1.2022:4], [PEP 5.4.2022:4].

Resolución.— Tener un conjunto X estructura de grupo respecto de una ley de composición $*$ significa que: 1.º, $*$ es una operación en X; 2.º, $*$ es asociativa en X; 3.º, existe el elemento neutro en X respecto de $*$, y 4.º, todo elemento de X tiene simétrico en X respecto de $*$; si además $*$ es conmutativa en X, decimos que X tiene estructura de grupo abeliano respecto de $*$.

Se trata de la suma módulo 6 que vistos los números como clases de equivalencia se define por $[x]_{(6)} +_6 [y]_{(6)} = [x + y]_{(6)}$, y en general, para un módulo m, $[x]_{(m)} +_m [y]_{(m)} = [x + y]_{(m)}$.

La tabla Cayley de esta ley es

$+_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Llamemos A al conjunto $\{0, 2, 4\}$; entonces:

I. como todos los resultados están en A, se trata de una ley de composición interna —una operación— en A, por lo que $(A, +_6)$ es un magma;

II. como la tabla es simétrica, dicha operación es conmutativa; por satisfacerse (0.º) y (1.º), $(A, +_6)$ es un magma abeliano;

III. demostramos que $+_6$ es asociativa de dos formas:

- *primera forma*:

por serlo la suma módulo 6 y, en general, módulo m, y ésta por serlo la suma de enteros, en efecto,

$$\begin{aligned}([x]_{(m)} +_m [y]_{(m)}) +_m [z]_{(m)} &= [x+y]_{(m)} +_m [z]_{(m)} && [\text{definición de } +_m]\\ &= [(x+y)+z]_{(m)} && [\text{definición de } +_m]\\ &= [x+(y+z)]_{(m)} && [\text{asociativa de } + \text{ en } \mathbb{Z}]\\ &= [x]_{(m)} +_m [y+z]_{(m)} && [\text{definición de } +_m]\\ &= [x]_{(m)} +_m ([y]_{(m)} +_m [z]_{(m)}) && [\text{definición de } +_m];\end{aligned}$$

- *segunda forma*:

  por un lado, si los tres términos intervinientes en la asociativa son iguales o si alguno es 0, su verificación es trivial; por otro, por ser $+_6$ conmutativa en A, se reduce el número de casos no triviales a sólo tres, cuyas verificaciones son:

  $$(2 +_6 2) +_6 4 = 4 +_6 4 = 2 = 2 +_6 0 = 2 +_6 (2 +_6 4),$$

  $$(2 +_6 4) +_6 4 = 0 +_6 4 = 4 = 2 +_6 2 = 2 +_6 (4 +_6 4);$$

por satisfacerse (0.º), (1.º) y (2.º), $(A, +_6)$ es un semigrupo abeliano;

IV. existe el elemento neutro de $+_6$ en A y es 0; en efecto, $0 +_6 0 = 0$, $0 +_6 2 = 2 +_6 0 = 2$ y $0 +_6 4 = 4 +_6 0 = 4$; por satisfacerse (0.º), (1.º), (2.º) y (3.º), $(A, +_6)$ es un monoide abeliano;

V. todo elemento de A tiene simétrico en A respecto de $+_6$; en efecto, $0' = 0$, $2' = 4$ [como $4 +_6 2 = 0$, lo es por la izquierda y como $2 +_6 4 = 0$, lo es por la derecha] y $4' = 2$ [como $2 +_6 4 = 0$, lo es por la izquierda y como $4 +_6 2 = 0$, lo es por la derecha]; por satisfacerse (0.º), (1.º), (2.º), (3.º) y (4.º), $(A, +_6)$ es un grupo abeliano. ■

Ejemplo 449

Sean $(G; *)$ un grupo abeliano y c un elemento de G distinto del neutro. Se define una segunda ley de composición diádica $\circledast$ en G de la forma

$$(\forall x, y \in G)\,(x \circledast y = x * y * c).$$

Demostremos que $(G; \circledast)$ es un grupo abeliano.

[EFO 4.6.2021:4]. *Cfr.* Anzola y Caruncho [140]: problema 10.14 (pág. 213).

Resolución.— Para demostrar que $(G; \circledast)$ es un grupo abeliano, debemos demostrar que $\circledast$ es una ley de composición interna en G que satisface las propiedades conmutativa, asociativa, que existe el elemento neutro en G respecto de $\circledast$ y que es tal que todo elemento de G tiene simétrico en G.

I. $\circledast$ es una *ley de composición interna* en G por serlo $*$. En efecto, $\forall x, y \in G$, como $(x * y) \in G$ y $c \in G$, entonces $(x * y) * c \in G$ y como $*$ es asociativa en G, $x * y * c \in G$.

II. $\circledast$ es *conmutativa* en G. En efecto, $\forall x, y \in G$,

$$\begin{aligned} x \circledast y &= x * y * c && \text{(por definición de } \circledast) \\ &= (x * y) * c && \text{(por ser } * \text{ asociativa en } G) \\ &= (y * x) * c && \text{(por ser } * \text{ conmutativa en } G) \\ &= y * x * c && \text{(por ser } * \text{ asociativa en } G) \\ &= x \circledast y && \text{(por definición de } \circledast) \end{aligned}$$

III. $\circledast$ es *asociativa* en G. En efecto, $\forall x, y, z \in G$,

$$\begin{aligned} (x \circledast y) \circledast z &= (x * y * c) \circledast z && \text{(por definición de } \circledast) \\ &= (x * y * c) * y * c && \text{(por definición de } \circledast) \\ &= x * (y * z * c) * c && \text{(por ser } * \text{ asociativa en } G) \\ &= x \circledast (y * z * c) && \text{(por definición de } \circledast) \\ &= x \circledast (y \circledast z) && \text{(por definición de } \circledast) \end{aligned}$$

IV. Existe el *elemento neutro* $e_\circledast$ de $\circledast$ en G. Veamos que

$$e_\circledast = c', \tag{17.7}$$

donde c' es el elemento simétrico de c en G respecto de $*$ (que existe porque $c \neq e_*$). Por ser $\circledast$ conmutativa en G, basta demostrar que c' es un neutro lateral; veamos que c' es el neutro por la derecha; en efecto, $\forall x \in G$,

$$\begin{aligned} x \circledast e_\circledast &= x * e_\circledast * c && \text{(por definición de } \circledast) \\ &= x * c' * c && \text{(por 17.7)} \\ &= x * (c' * c) && \text{(por ser } * \text{ asociativa en } G) \\ &= x * e_* && \text{(por definición de simétrico —} e_* \text{ es el neutro de } * \text{ en } G\text{—)} \\ &= x && \text{(por ser } e_* \text{ el neutro de } * \text{ en } G) \end{aligned}$$

V. Todo elemento x de G tiene *simétrico* x^{-1} en G respecto de $\circledast$. Veamos que

$$x^{-1} = x' * c' * c', \tag{17.8}$$

donde x' es el elemento simétrico de x y c' el de c, respecto de $*$, en G (recordemos que c es un elemento «fijo» de C). Por ser $\circledast$ conmutativa en G, basta demostrar que x tiene un simétrico

lateral; veamos que $x' * c' * c'$ es el simétrico por la derecha de x; en efecto, $\forall x \in G$,

$$\begin{aligned} x \circledast x^{-1} &= x * x^{-1} * c && \text{(por definición de } \circledast) \\ &= x * (x' * c' * c') * c && \text{(por (17.8))} \\ &= (x * x') * c' * (c' * c) && \text{(por ser } * \text{ asociativa en } G) \\ &= e_* * c' * e_* && \text{(por definición de simétrico)} \\ &= c' && \text{(por definición de elemento neutro)} \\ &= e_\circledast && \text{(por (17.7))} \end{aligned}$$

■

Ejemplo 450

En el conjunto $2\mathbb{Z}$ de los números enteros pares se define, $\forall 2m, 2n \in 2\mathbb{Z}$, la ley de composición, $2m * 2n = 2m + 2n + 2mn$, siendo la suma y la multiplicación las habituales entre enteros (observemos que cualquier número de $2\mathbb{Z}$, por ser par, puede escribirse como $2k$, para un cierto entero k —por ejemplo, escribimos $2 \cdot 5 \in 2\mathbb{Z}$ en vez de $10 \in 2\mathbb{Z}$—). Demostremos que:

0. $(2\mathbb{Z}; *)$ es un monoide abeliano;
1. $(2\mathbb{Z}; *)$ no es un grupo.

[EFE 7.7.2021:4]. *Cfr.* Anzola y Caruncho [140]: problema 10.24 (pág. 221).

Resolución.—

0. Para demostrar que $(2\mathbb{Z}; *)$ es un monoide abeliano, debemos demostrar que $*$ es una ley de composición interna en $2\mathbb{Z}$ que satisface las propiedades conmutativa, asociativa y que existe el elemento neutro en $2\mathbb{Z}$ respecto de $*$.

Sabemos que $(\mathbb{Z}; +, \cdot)$ es un dominio de integridad, esto es, un anillo (unitario) abeliano sin divisores de cero. En particular, en $\mathbb{Z}$, por una parte, $+$ es una ley de composición interna, conmutativa, asociativa, con elemento neutro 0 y tal que todo entero n tiene simétrico (su opuesto, $-n$); por la otra parte, $\cdot$ es una ley de composición interna, conmutativa, asociativa, con elemento neutro 1 y distributiva respecto de $+$.

1. $*$ es una *ley de composición interna* en $2\mathbb{Z}$ por serlo la suma y producto ordinarios en $\mathbb{Z}$. En efecto, para cualesquiera $2m$ y $2n$ de $2\mathbb{Z}$,

$$\begin{aligned} 2m * 2n &= 2m + 2n + 2mn && \text{(por definición de } *) \\ &= (2m + n) + 2mn && \text{(por asociativa de } + \text{ en } \mathbb{Z}) \\ &= 2(m + n) + 2mn && \text{(por distributiva de } \cdot \text{ respecto de } + \text{ en } \mathbb{Z}) \\ &= 2((m + n) + mn) && \text{(por distributiva de } \cdot \text{ respecto de } + \text{ en } \mathbb{Z}) \\ &= 2(m + n + mn) && \text{(por asociativa de } + \text{ en } \mathbb{Z}) \end{aligned}$$

$$\in 2\mathbb{Z}. \qquad \text{(por definición de } 2\mathbb{Z} \text{ —} 2m * 2n \text{ es par—)}$$

II. $*$ es *conmutativa* en $2\mathbb{Z}$. En efecto, para cualesquiera $2m$ y $2n$ de $2\mathbb{Z}$,

$$\begin{aligned}
2m * 2n &= 2m + 2n + 2mn && \text{(por definición de } *)\\
&= (2m + 2n) + 2mn && \text{(por asociativa de } + \text{ en } \mathbb{Z})\\
&= (2n + 2m) + 2mn && \text{(por conmutativa de } + \text{ en } \mathbb{Z})\\
&= (2n + 2m) + 2(mn) && \text{(por asociativa de } \cdot \text{ en } \mathbb{Z})\\
&= (2n + 2m) + 2(nm) && \text{(por conmutativa de } \cdot \text{ en } \mathbb{Z})\\
&= 2n + 2m + 2nm && \text{(por asociativa de } + \text{ y } \cdot \text{ en } \mathbb{Z})\\
&= 2n * 2m && \text{(por definición de } *)
\end{aligned}$$

III. $*$ es *asociativa* en $2\mathbb{Z}$. En efecto, para cualesquiera $2m, 2n, 2\tilde{n}$ de $2\mathbb{Z}$,

$$\begin{aligned}
(2m * 2n) * 2\tilde{n} &= (2m + 2n + 2mn) * 2\tilde{n} && \text{(por definición de } *)\\
&= 2(m + n + mn) * 2\tilde{n} && \text{(por distributiva de } \cdot \text{ respág. de } + \text{ en } \mathbb{Z})\\
&= 2(m + n + mn) + 2\tilde{n} + 2(m + n + mn)\tilde{n} && \text{(por definición de } *)\\
&= (2m + 2n + 2mn) + 2\tilde{n} + (2m\tilde{n} + 2n\tilde{n} + 2mn\tilde{n}) && \text{(por distributiva de } \cdot \text{ respág. de } + \text{ en } \mathbb{Z})\\
&= 2m + 2n + 2mn + 2\tilde{n} + 2m\tilde{n} + 2n\tilde{n} + 2mn\tilde{n} && \text{(por asociativa de } + \text{ en } \mathbb{Z})\\
&= 2m + 2n + 2\tilde{n} + 2n\tilde{n} + 2mn + 2m\tilde{n} + 2mn\tilde{n} && \text{(por asociativa y conmutativa de } + \text{ en } \mathbb{Z})\\
&= 2m + (2n + 2\tilde{n} + 2n\tilde{n}) + (2mn + 2m\tilde{n} + 2mn\tilde{n}) && \text{(por asociativa de } + \text{ en } \mathbb{Z})\\
&= 2m + 2(n + \tilde{n} + n\tilde{n}) + 2m(n + \tilde{n} + n\tilde{n}) && \text{(por distributiva de } \cdot \text{ respág. de } + \text{ en } \mathbb{Z})\\
&= 2m * 2(n + \tilde{n} + n\tilde{n}) && \text{(por definición de } *)\\
&= 2m * (2n + 2\tilde{n} + 2n\tilde{n}) && \text{(por distributiva de } \cdot \text{ respág. de } + \text{ en } \mathbb{Z})\\
&= 2m * (2n * 2\tilde{n}) && \text{(por definición de } *)
\end{aligned}$$

IV. Existe el *elemento neutro* e_* de $*$ en $2\mathbb{Z}$. Veamos que

$$e_* = 0 = 2 \cdot 0, \tag{17.9}$$

donde 0 es el elemento neutro de $+$ en $\mathbb{Z}$. Por ser $*$ conmutativa en $2\mathbb{Z}$, basta demostrar que 0 es un neutro lateral; veamos que 0 es el neutro por la derecha; en efecto, $\forall 2m \in 2\mathbb{Z}$,

$$\begin{aligned}
2m * e_* &= 2m * 2 \cdot 0 && \text{(por 17.9)}\\
&= 2m + 2 \cdot 0 + 2 \cdot m \cdot 0 && \text{(por definición de } *)\\
&= 2m + 0 + 0 && \text{(por ser } 0 \text{ absorbente para } \cdot \text{ en } \mathbb{Z})\\
&= 2m && \text{(por ser } 0 \text{ el neutro de } + \text{ en } \mathbb{Z})
\end{aligned}$$

Por un teorema, sabemos que en un monoide el elemento neutro es único, luego, en efecto, 0 es el neutro de $*$ en $2\mathbb{Z}$.

1. Visto lo demostrado en el apartado anterior, para demostrar que $(2\mathbb{Z}; *)$ no es un grupo abeliano, debemos demostrar que $*$ es tal que no todo elemento de $2\mathbb{Z}$ tiene simétrico en $2\mathbb{Z}$ respecto de $*$.

En efecto, de existir el *simétrico* $(2m)^{-1}$ de $2m$ en $2\mathbb{Z}$ respecto de $*$, sería de la forma $2k$ con k entero (por tener que pertenecer a $2\mathbb{Z}$); por otro lado, por ser $*$ conmutativa en $2\mathbb{Z}$, bastaría demostrar que $2m$ tiene un simétrico lateral; buscándolo por la derecha, $\forall 2m \in 2\mathbb{Z}$, como por definición de $*$, $2m * 2k = 2m + 2k + 2mk$, nos interesa encontrar un k entero tal que

$$2m + 2k + 2mk = 0$$

esto ocurre si, y sólo si,

$$\begin{aligned}
& 2m + (2k + 2mk) = 0 && \text{(por asociativa de } + \text{ en } \mathbb{Z})\\
\leftrightarrow\ & 2m + (2 + 2m)k = 0 && \text{(por distributiva de } \cdot \text{ respág. de } + \text{ en } \mathbb{Z})\\
\leftrightarrow\ & k = -\frac{2m}{2+2m} && \text{(por ser } (\mathbb{Q}; +, \cdot) \text{ un cuerpo)}\\
\leftrightarrow\ & k = -\frac{m}{1+m} && \text{(simplificando en el cuerpo } (\mathbb{Q}; +, \cdot))
\end{aligned}$$

de donde, por ejemplo, $2 = 2 \cdot 1$ no tiene simétrico en $2\mathbb{Z}$, pues si $m = 1$, $k = -\frac{1}{2}$, pero, entonces, $2k = -1$, el obligado candidato a simétrico de 2, no pertenece a $2\mathbb{Z}$ (-1 no es par). ■

Observación 17.5.2.— En 0.iv, caso de no haber intuido que $e_* = 0$, pudiésemos haber planteado resolver la ecuación $2m * e_* = 2m$, siendo $2m \in 2\mathbb{Z}$, de donde,

$$\begin{aligned}
2m * e_* = 2m & \leftrightarrow 2m + 2e_* + 2me_* = 2m && \text{(por definición de } *)\\
& \leftrightarrow (-2m + 2m) + 2e_* + 2me_* = -2m + 2m && \text{(por ley de cancelación de } + \text{ en } \mathbb{Z}\\
& && \text{ y por asociativa de } + \text{ en } \mathbb{Z})\\
& \leftrightarrow 0 + 2e_* + 2me_* = 0 && \text{(por ser } -2m \text{ el simétrico de } 2m \text{ en } \mathbb{Z})\\
& \leftrightarrow 2e_* + 2me_* = 0 && \text{(por ser 0 el neutro de } + \text{ en } \mathbb{Z})\\
& \leftrightarrow (2 + 2m)e_* = 0 && \text{(por distributiva de } \cdot \text{ respág. de } + \text{ en } \mathbb{Z})\\
& \leftrightarrow e_* = 0 && (2 + 2m \neq 0 \text{ y } (\mathbb{Z}; \cdot) \text{ no tiene divisores de cero})
\end{aligned}$$

Observación 17.5.3.— Respecto a 1., la ecuación $k = -\frac{m}{1+m}$ tiene, de hecho, sólo dos soluciones en $\mathbb{Z}$, a saber, $\langle k, m \rangle = \langle 0, 0 \rangle$ y $\langle k, m \rangle = \langle -2, -2 \rangle$, de donde $2k = 0$ y $2(-2) = -4$, respectivamente y, por tanto, únicamente dos elementos de $2\mathbb{Z}$ tienen simétrico respecto de $*$, 0 y -4, cuyos simétricos son $0^{-1} = 0$ y $(-4)^{-1} = -4$, respectivamente.

Ejemplo 451

Sea C un conjunto, 2^C su conjunto potencia y $\triangle$ designa la diferencia simétrica de conjuntos. Demostremos que $(2^C; \triangle)$ tiene estructura de grupo abeliano.

Sugerencia.— El ejemplo 302 (pág. 558 de esta edición) es de ayuda.

[SEP 12.5.2022:4].

Resolución.— Para demostrar que $(2^C; \triangle)$ es un grupo abeliano, debemos demostrar que $\triangle$ es una ley de composición interna en 2^C que satisface las propiedades conmutativa, asociativa, que existe el elemento neutro en 2^C respecto de $\triangle$ y que es tal que todo elemento de 2^C tiene simétrico en 2^C.

Dados dos conjuntos X e Y, se define la diferencia simétrica a partir de la diferencia $\setminus$ y de la unión $\cup$ entre conjuntos, $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$, lo que, por definición de $\setminus$, resulta ser igual a $(X \cap Y^{\complement}) \cup (X^{\complement} \cap Y)$.

También usaremos el resultado provisto por el ejemplo 302 (pág. 558 de esta edición):

$$(X \triangle Y)^{\complement} = (X \cap Y) \cup (X^{\complement} \cap Y^{\complement}) \tag{17.10}$$

0. $\triangle$ es una *ley de composición interna* en 2^C por serlo $\cup$ y $\cap$. En efecto, $X \triangle Y = (X \cap Y^{\complement}) \cup (X^{\complement} \cap Y)$ y como, por definición de intersección, el primero está incluido en X y el segundo en Y, y tanto X como Y son subconjuntos de C (y su unión también lo es, por definición de unión), por tanto, $\forall X, Y \in 2^C$, $X \triangle Y$ es subconjunto de C, es decir, $X \triangle Y \in 2^C$.

1. $\triangle$ es *conmutativa* en 2^C. En efecto, $\forall X, Y \in 2^C$,

$$\begin{aligned} X \triangle Y &= (X \setminus Y) \cup (Y \setminus X) && \text{(por definición de } \triangle) \\ &= (Y \setminus X) \cup (X \setminus Y) && \text{(por ser } \cup \text{ conmutativa en } 2^C) \\ &= Y \triangle X && \text{(por definición de } \triangle) \end{aligned}$$

2. $\triangle$ es *asociativa* en 2^C.

[EFO 27.5.2025:4bII] (asociativa), [EFE 18.6.2025:4bII] (asociativa).

En efecto, $\forall X, Y, Z \in 2^C$,

$$\begin{aligned} &(X \triangle Y) \triangle Z \\ &= ((X \triangle Y) \setminus Z) \cup (Z \setminus (X \triangle Y)) && \text{(por definición de } \triangle) \end{aligned}$$

$$
\begin{aligned}
&= ((X \triangle Y) \cap Z^{\complement}) \cup (Z \cap (X \triangle Y)^{\complement}) && \text{(por definición de } \setminus) \\
&= (((X \setminus Y) \cup (Y \setminus X)) \cap Z^{\complement}) \cup (Z \cap ((X \cap Y) \cup (X^{\complement} \cap Y^{\complement}))) && \text{(por def. de } \triangle \text{ y 17.10)} \\
&= (((X \cap Y^{\complement}) \cup (Y \cap X^{\complement})) \cap Z^{\complement}) \cup (Z \cap ((X \cap Y) \cup (X^{\complement} \cap Y^{\complement}))) && \text{(por definición de } \setminus) \\
&= (X \cap Y^{\complement} \cap Z^{\complement}) \cup (Y \cap X^{\complement} \cap Z^{\complement}) \cup (Z \cap X \cap Y) \cup (Z \cap X^{\complement} \cap Y^{\complement}) && \text{(por distributiva de } \cap \text{ respecto de } \cup) \\
&= (X \cap (Y \cap Z)) \cup (X \cap (Y^{\complement} \cap Z^{\complement})) \cup ((Y \cap Z^{\complement}) \cap X^{\complement}) \cup ((Z \cap Y^{\complement}) \cap X^{\complement}) && \text{(por conmutativa y asociativa de } \cup \text{ y } \cap) \\
&= (X \cap ((Y \cap Z) \cup (Y^{\complement} \cap Z^{\complement}))) \cup (((Y \cap Z^{\complement}) \cup (Z \cap Y^{\complement})) \cap X^{\complement}) && \text{(por distributiva de } \cap \text{ respecto de } \cup) \\
&= (X \cap (Y \triangle Z)^{\complement}) \cup ((Y \triangle Z) \cap X^{\complement}) && \text{(por 17.10 y def. de } \triangle) \\
&= (X \setminus (Y \triangle Z)) \cup ((Y \triangle Z) \setminus X) && \text{(por definición de } \setminus) \\
&= X \triangle (Y \triangle Z). && \text{(por definición de } \triangle)
\end{aligned}
$$

3. Existe el *elemento neutro* $e_{\triangle}$ de $\triangle$ en 2^C. Veamos que

$$e_{\triangle} = \emptyset, \tag{17.11}$$

donde $\emptyset$ es el conjunto vacío. Por ser $\triangle$ conmutativa en 2^C, basta demostrar que $\emptyset$ es un neutro lateral; veamos que $\emptyset$ es el neutro por la derecha; en efecto, $\forall X \in 2^C$,

$$
\begin{aligned}
X \triangle e_{\triangle} &= (X \setminus e_{\triangle}) \cup (e_{\triangle} \setminus X) && \text{(por definición de } \triangle) \\
&= (X \setminus \emptyset) \cup (\emptyset \setminus X) && \text{(por 17.11)} \\
&= (X \cap \emptyset^{\complement}) \cup (\emptyset \cap X^{\complement}) && \text{(por def. de } \setminus) \\
&= (X \cap \mathcal{U}) \cup (\emptyset \cap X^{\complement}) && \text{(por defs. de } \emptyset \text{ y } \mathcal{U}) \\
&= (X \cap \mathcal{U}) \cup \emptyset && \text{(por ley de dominación)} \\
&= X \cup \emptyset && \text{(por ley de identidad)} \\
&= X, && \text{(por ley de identidad)}
\end{aligned}
$$

4. Todo elemento X de 2^C tiene *simétrico* X^{-1} en 2^C respecto de $\triangle$. Veamos que

$$X^{-1} = X, \tag{17.12}$$

esto es, todo elemento es su propio simétrico. Por ser $\triangle$ conmutativa en 2^C, basta demostrar que X tiene un simétrico lateral; veamos que X es el simétrico por la derecha de X; en efecto, $\forall X \in 2^C$,

$$
\begin{aligned}
X \triangle X^{-1} &= (X \setminus X^{-1}) \cup (X^{-1} \setminus X) && \text{(por definición de } \triangle) \\
&= (X \setminus X) \cup (X \setminus X) && \text{(por (17.12))} \\
&= (X \cap X^{\complement}) \cup (X \cap X^{\complement}) && \text{(por definición de } \setminus)
\end{aligned}
$$

$$= \emptyset \cup \emptyset \qquad \text{(por ley de complemento)}$$
$$= \emptyset \qquad \text{(por ley de identidad)}$$
$$= e_{\triangle} \qquad \text{(por (17.11))}$$ ■

Actividad 17.0

Hagamos todo lo propuesto en el ejemplo anterior para la estructura $\left(2^{\{x,y\}}; \triangle^{\complement}\right)$, siendo $\triangle^{\complement}$ la operación complementario de la diferencia simétrica.

Teorema 17.17 (Algunas propiedades)
Sean $(G; *)$ un grupo. Entonces, $\forall x, y \in G$ se satisface:
0.º, $(x * y)' = y' * x'$;
1.º, $(x')' = x$;
2.º, x es regular.

Ejemplo 452

Sea $*$ una operación en un conjunto X en el que existe elemento neutro para $*$ y todo elemento de X tiene simétrico y satisface para todo $x, y \in X$, $x * y = y * x$, ¿cuál de las siguientes afirmaciones es verdadera?

a. $*$ es conmutativa y asociativa en X.
b. $*$ es conmutativa en X, pero no asociativa.
c. $*$ es conmutativa en X y puede que asociativa.
d. $*$ ni es conmutativa ni asociativa en X.

[TT], [EFEC 29.1.2025:6] (tipo test).

Resolución.— Según el enunciado, $*$ es conmutativa en X. Analicemos las opciones.

a. No es verdadera; un contraejemplo es la operación diádica $x*y = |x-y|$ en $\mathbb{N}$, que es conmutativa trivialmente, el elemento neutro es 0, todo elemento es su propio simétrico —$x*x = |x-x| = 0$— y no es asociativa —por ejemplo, $(1*1)*2 = ||1-1|-2| = 2 \neq 0 = |1-|1-2|| = (1*(1*2))$—.

b. No es verdadera; un contraejemplo es la operación diádica $x * y = x \veebar y$ en $\{0, 1\}$, que es conmutativa $x * y = x \veebar y = y \veebar x = y * x$, el elemento neutro es 0, el simétrico de x es x, y es asociativa —pues $(x \veebar y) \veebar z = x \veebar (y \veebar z)$ es una fórmula válida—.

c. Es verdadera; sí es conmutativa por el enunciado y pudiese ser asociativa —precisamente en los apartados anteriores hemos visto ejemplos de serlo (apdo. b) y no serlo (apdo. a)—.

d. No es verdadera, pues sí que es conmutativa, por el enunciado.

Solución.— Opción c. ■

§ 17.5.0 Subgrupo

Definición 17.22.— Sean $(G;*)$ un grupo y $S \subseteq G$. Decimos que $(S;*)$ es un *subgrupo* del grupo $(G;*)$, precisamente si $(S;*)$ es un grupo.

Teorema 17.18 (Caracterización de subgrupo)
Sean $(G;*)$ un grupo y $S \subseteq G$, $S \neq \emptyset$. Entonces, $(S;*)$ es subgrupo de $(G;*)$, precisamente si

$$(\forall x, y \in S)(x * y \in S), \text{ y}$$
$$(\forall x \in S)(x' \in S),$$

esto es, si, y sólo si,

$$(\forall x, y \in S)(x * y' \in S).$$

Definición 17.23.— Dado un grupo $(G;*)$, llamamos *subgrupos impropios* a $(G;*)$ y $(\{e\};*)$ y *subgrupo propio* a cualquier otro.

Teorema 17.19
Los subgrupos de un grupo forman un retículo con $(\{e\};*)$ el mínimo y $(G;*)$ el máximo, pudiendo representarse mediante un diagrama de HASSE.

Teorema 17.20
El centro de un grupo es un subgrupo suyo.

Teorema 17.21
Se satisface:

0. si en un grupo todos sus elementos son idempotentes, entonces dicho grupo es abeliano;
1. si $(G;*)$ es un grupo, entonces es abeliano si, y sólo si, $(\forall x, y \in G)((x * y)^2 = x^2 * y^2)$;
2. si un grupo es abeliano, entonces todos sus subgrupos son abelianos.

Teorema 17.22
Se satisface:

0. la intersección de subgrupos de un mismo grupo es un subgrupo de dicho grupo;
1. la unión de subgrupos no es en general ni siquiera un grupo.

§ 17.5.1 Subgrupo normal

Definición 17.24.— Sean $(G;*)$ un grupo, $(S;*)$ un subgrupo suyo y $x \in G$. Llamamos *clase de G a la izquierda módulo S* al conjunto

$$xS = \{y \in G : (\forall s \in S)(y = x * s)\}$$

y *clase de G a la derecha módulo S* al conjunto

$$Sx = \{y \in G : (\forall s \in S)(y = s * x)\}.$$

Definición 17.25.— Sean $(G;*)$ un grupo y $(S;*)$ un subgrupo suyo. Decimos que $(S;*)$ es un *subgrupo normal* (o, sinónimamente, *subgrupo invariante*), y notamos $S \trianglelefteq G$, precisamente si

$$(\forall x \in G)(xS = Sx).$$

Teorema 17.23
Todo subgrupo de un grupo abeliano es normal.

Demostración.— Sea cual sea el subgrupo S de un grupo abeliano G, $xS = \{x * s : sS\} = \{s * x : sS\} = Sx$, precisamente por la conmutatividad de $*$. ■

Ejemplo 453

¿Cuáles son los subgrupos normales de $(\mathbb{Z};+)$?

Resolución.— Como $(\mathbb{Z};+)$ es un grupo abeliano, todos los subgrupos de $\mathbb{Z}$ —que son precisa y únicamente los de la forma $\{nx : x \in \mathbb{Z}\}$— son subrupos normales. ■

§ 17.5.2 Homomorfismo de grupos

Definición 17.26.— Sean $(G_0;*)$ y $(G_1;\circ)$ dos grupos y $f : G_0 \longrightarrow G_1$ una aplicación. Decimos que f es un *homomorfismo de grupos*, precisamente si lo es como homomorfismo de magmas, esto es, precisamente si $\forall a, b \in G_0$ se satisface

$$f(a * b) = f(a) \circ f(b).$$

Definición 17.27.— Sean $(G_0;*)$ y $(G_1;\circ)$ dos grupos y $f : G_0 \longrightarrow G_2$ un homomorfismo de grupos. Llamamos *núcleo de f*, y lo designamos por $\ker f$, al conjunto

$$\ker f = \{x \in G_0 : f(x) = e_\circ\}.$$

Teorema 17.24
Sean $(G_0;*)$ y $(G_1;\circ)$ dos grupos y $f : G_0 \longrightarrow G_1$ un homomorfismo de grupos. Entonces, $\forall a \in G_0$ se satisface que:

0. si e es el neutro de $(G_0;*)$, entonces $f(e)$ es el neutro de $(G_1;\circ)$;
1. si x' es el simétrico de x para $*$, entonces $f(x')$ es el simétrico de $f(x)$ para $\circ$;
2. $(f(G_0);\circ)$ es grupo;
3. $\ker f$ es un subgrupo normal de $(G_0;*)$;
4. f es monomorfismo si, y sólo si, $\ker f = \{e\}$.

Definición 17.28 (Grupo cociente módulo un subgrupo normal).— Sean $(G;*)$ un grupo y $(S;*)$ un subgrupo normal suyo. Sea $C = \{aS : a \in G\}$ el conjunto de las clases de G módulo S, que es una partición de G. Llamamos *grupo cociente* de G módulo S y lo designamos por G/S al grupo $(C;\cdot)$, donde $\cdot$ se define, $\forall aS, bS \in C$, por $aS \cdot bS = (a \cdot b)S$.

Teorema 17.25 (Descomposición canónica de un homomorfismo de grupos)
Sean $(G_0;*)$ y $(G_1;\circ)$ dos grupos y $f : G_0 \longrightarrow G_1$ un homomorfismo de grupos. Entonces, la descomposición canónica de f es $f = n \circ g \circ i$, esto es,

$$\begin{array}{ccc} G_0 & \xrightarrow{f} & G_1 \\ \downarrow n & & \uparrow i \\ G_0/\ker f & \xrightarrow{g} & f(G_0) \end{array}$$

donde:
n es el epimorfismo definido por $n(x) = x \ker f$;
g es el isomorfismo definido por $g(x \ker f) = f(x)$, e
i es el monomorfismo definido por $i(x) = x$.

§ 17.5.3 Grupo finito

Definición 17.29.— Llamamos *grupo finito* a cualquier grupo que conste de un número finito de elementos.

Definición 17.30.— Llamamos *orden de un grupo* al número de elementos del grupo.

Definición 17.31.— Sean $(G;*)$ un grupo y $x \in G$. Llamamos *orden* (finito) *del elemento* x al menor $n \in \mathbb{N}$ tal que

$$x^n = e,$$

donde $x^n = x * \overset{n}{\smile} \cdots * x$. Caso de que no exista tal $n \in \mathbb{N}$ para $x \in G$, decimos que x tiene *orden infinito*.

Definición 17.32.— Sean $(G; *)$ un grupo y $x \in G$. Decimos que x es un *elemento de torsión* del grupo precisamente si x tiene orden finito.

Definición 17.33.— Decimos que un grupo $(G; *)$ es un *grupo de torsión* precisamente si todos sus elementos son elementos de torsión. Caso de que el único elemento de torsión sea el elemento neutro decimos de $(G; *)$ que es un *grupo libre de torsión*.

Teorema 17.26 (Teorema de LAGRANGE)
El orden de un grupo finito es múltiplo del orden de cualquier subgrupo suyo.

Definición 17.34.— Sean $(G; *)$ un grupo finito y $(S; *)$ un subgrupo suyo. Llamamos índice de S a:

$$\mathrm{i}(S) = \frac{\mathrm{o}(G)}{\mathrm{o}(S)}.$$

Observación 17.5.4.— Notemos que debido al teorema de LAGRANGE, el índice de cualquier subgrupo es un número natural.

Teorema 17.27
Sean $(G; *)$ un grupo finito y $(S; *)$ un subgrupo suyo. Se satisface que

$$\text{si } \mathrm{i}(S) = 2, \text{ entonces } (S; *) \text{ es un subgrupo normal de } (G; *).$$

§ 17.5.4 Grupo cíclico

Definición 17.35.— Sean $(G; *)$ un grupo y S un subconjunto finito de G. Decimos que $(G; *)$ es un *grupo finitamente generado* por S precisamente si todo elemento de G puede obtenerse como resultado de la operación diádica sobre elementos de S o sobre elementos ya generados. Si S es de cardinal uno, decimos que $(G; *)$ es un *grupo monógeno*.

Observación 17.5.5.— Si $(G; *)$ es un grupo finitamente generado por S, entonces $(G; *)$ es el menor grupo que contiene a S.

Definición 17.36.— Decimos que $(G; *)$ es un *grupo cíclico* precisamente si es un grupo monógeno y finito.

Teorema 17.28
Todo grupo cíclico es conmutativo.

Ejemplo 454

Sean la figura plana $\vee$ y el conjunto de rotaciones $R = \{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\}$ en el plano euclideo E_2.

Las rotaciones son en sentido anti-horario, el estándar en matemáticas; además, consideramos que el eje de rotación pasa por el centroide de la figura plana.

Estas rotaciones son un caso particular de transformaciones del plano euclideo, esto es, de aplicaciones $R : E_2 \longrightarrow E_2$. Estas rotaciones, aplicadas a la figura $\vee$, originan las siguientes transformaciones isométricas por rotación de la misma que muestra la columna 0; en las siguientes columnas mostramos las rotaciones sobre rotaciones (composición de rotaciones):

	$\vee$	$<$	$\wedge$	$>$
R_0	$\vee$	$<$	$\wedge$	$>$
$R_{\pi/2}$	$>$	$\vee$	$<$	$\wedge$
R_π	$\wedge$	$>$	$\vee$	$<$
$R_{3\pi/2}$	$<$	$\wedge$	$>$	$\vee$

Consideremos el conjunto $R = \{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\}$ y la ley de composición diádica $\circ$, la composición de rotaciones en R, que es una operación en R. Se tiene que $(R; \circ)$ es un grupo cíclico de orden cuatro que únicamente tiene un subgrupo propio.

[Cubit 92].

Resolución.— En efecto, tiene 4 elementos, luego, de ser grupo, es finito y ése es su orden. Veamos que es grupo. He aquí la *tabla de* CAYLEY de la ley de composición $\circ$ en R:

$\circ$	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$
R_0	R_0	$R_{\pi/2}$	R_π	$R_{3\pi/2}$
$R_{\pi/2}$	$R_{\pi/2}$	R_π	$R_{3\pi/2}$	R_0
R_π	R_π	$R_{3\pi/2}$	R_0	$R_{\pi/2}$
$R_{3\pi/2}$	$R_{3\pi/2}$	R_0	$R_{\pi/2}$	R_π

Se satisface:

I. la ley de composición $\circ$ es una operación en R pues todos los resultados son elementos de R;

II. la operación $\circ$ es asociativa en R, ya que las rotaciones son aplicaciones y la composición de aplicaciones es asociativa (o también pudiésemos comprobar todas las tríadas);[9]

[9] Más adelante, expresaremos la composición de rotaciones como producto de matrices, por lo que podremos razonar también cómo la composición de rotaciones es asociativa por serlo el producto de matrices.

III. la operación $\circ$ es conmutativa en R, puesto que la tabla es simétrica respecto de la diagonal principal;

IV. el elemento neutro para $\circ$ en R es R_0, ya que, por un lado, R_0 es neutro por la izquierda, pues la fila cero es copia de la fila de cabecera y, por otro, R_0 es neutro por la derecha, pues la columna cero es copia de la columna de cabecera;

V. todo elemento de R es simetrizable por $\circ$ —en la tabla, para una rotación determinada, sólo hay que buscar qué otra rotación compuesta con ella da el neutro (por ejemplo, el simétrico de $R_{\pi/2}$ es $R_{3\pi/2}$ porque $R_{\pi/2} \circ R_{3\pi/2} = R_{3\pi/2} \circ R_{\pi/2} = R_0$)—.

Además, es un grupo monógeno, esto es, generado por uno de sus elementos; concretamente tanto $R_{\pi/2}$ como $R_{3\pi/2}$ son capaces de generar todo el grupo. Por ejemplo:

$$\begin{aligned} R_{\pi/2} \circ R_{\pi/2} &= R_{\pi} \\ R_{\pi/2} \circ R_{\pi} &= R_{3\pi/2} \\ R_{\pi/2} \circ R_{3\pi/2} &= R_0 \end{aligned}$$

Como es finito, es un grupo cíclico de orden 4 y, por tanto, como mencionaremos en la observación 17.6.3 (pág. 883 de esta edición), isomorfo al grupo cíclico C_4, esto es, $(R; \circ)$ es un modelo para C_4.

Las estructuras $(R; \circ)$ y $(\{R_0\}\,; \circ)$ son subgrupos impropios. El único subgrupo propio es $(S = \{R_0, R_\pi\}\,; \circ)$ (no hay más subgrupos propios porque de contener cualquier subgrupo $(S', \circ)$ a $R_{\pi/2}$ o a $R_{3\pi/2}$, al ser éstos generadores de $(R, \circ)$, todas las rotaciones de R estarían en S'.

Que $(S, \circ)$ sea un subgrupo de $(R, \circ)$ se deduce del teorema de caracterización de subgrupos (teorema 17.18 [pág. 863 de esta edición]), ya que es cierto que $(\forall x, y \in S)(x * y' \in S)$, pues S sólo tiene dos elementos, R_0 y R_π, siendo ambas sus propios simétricos, $R_0' = R_0$ y $R_\pi' = R_\pi$, así que:

x	y	y'	$x * y'$
R_0	R_π	R_π	$R_0 \circ R_\pi = R_\pi$
R_π	R_0	R_0	$R_\pi \circ R_0 = R_\pi$

El diagrama de Hasse del retículo de sus subgrupos es

$$\begin{array}{c} \{R_0, R_{\pi/2}, R_\pi, R_{3\pi/2}\} \\ | \\ \{R_0, R_\pi\} \\ | \\ \{R_0\} \end{array}$$

■

Actividad 17.1

Consideremos como figura el trípode —tres segmentos a 90, 210 y 330 grados ($\pi/2$, $7\pi/6$ y $11\pi/6$ radianes, respectivamente)—, el conjunto de rotaciones $R = \{R_0, R_{2\pi/3}, R_{4\pi/3}\}$ (esto es, de 0, 120 y 240 grados) y, representando por $F_{y=ax+b}$ la reflexión de eje la recta $y = ax + b$, el conjunto de reflexiones $F = \{F_{x=0}, F_{x=y\sqrt{3}}, F_{x=-y\sqrt{3}}\}$ (esto es, el conjunto de reflexiones según sus tres segmentos). Consideremos la operación diádica $\circ$, composición de transformaciones (rotaciones o reflexiones) sobre $R \cup F$. Demostremos (*cfr. supra* ejemplo 454 [pág. 867 de esta edición]) que $(R \cup F; \circ)$ es un grupo y estudiémoslo. Observemos, por ejemplo, que el trípode presenta simetría axial (especular) para cada uno de sus segmentos considerados como ejes de simetría:



[Cubit 93].

Actividad 17.2

Estudiemos lo que sucede para el trisquel* —trípode con los segmentos acodados en ángulo recto y sentido levógiro— con todas o algunas de las isometrías consideradas en Cubit 93 (las tres rotaciones y las tres reflexiones), esto es, estudiemos la estructura de $(S; \circ)$ para algún $S \subseteq R \cup F$.†

[Cubit 94].

* *Vid. v. gr.* https://es.wikipedia.org/wiki/Trisquel.
† *Cfr. v. gr.* https://en.wikipedia.org/wiki/Chirality_(mathematics).

§ 17.5.5 Residuos

El conjunto de enteros $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ recibe el nombre de *el menor sistema de residuos módulo m*. Definiendo las operaciones, $\forall x, y \in \mathbb{Z}_m$,

$$x +_m y = (x + y) \text{ mód } m,$$
$$x \cdot_m y = (x \cdot y) \text{ mód } m,$$

se satisface que:

- $(\mathbb{Z}_m; +_m)$ tiene estructura de grupo abeliano;
- $(\mathbb{Z}_m; \cdot_m)$ tiene estructura de monoide abeliano;

- $(\mathbb{Z}_m \setminus \{0\}; \cdot_m)$ tiene estructura de grupo abeliano.

  Las tablas de Cayley de estas operaciones son las siguientes.

$+_m$	0	1	2	$\dots$	$m-3$	$m-2$	$m-1$
0	0	1	2	$\dots$	$m-3$	$m-2$	$m-1$
1	1	2	3	$\dots$	$m-2$	$m-1$	0
2	2	3	4	$\dots$	$m-1$	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$m-3$	$m-3$	$m-2$	$m-1$	$\dots$	$m-6$	$m-5$	$m-4$
$m-2$	$m-2$	$m-1$	0	$\dots$	$m-5$	$m-4$	$m-3$
$m-1$	$m-1$	0	1	$\dots$	$m-4$	$m-3$	$m-2$

$\cdot_m$	0	1	2	$\dots$	$m-3$	$m-2$	$m-1$
0	0	0	0	$\dots$	0	0	0
1	0	1	2	$\dots$	$m-3$	$m-2$	$m-1$
2	0	2	4	$\dots$	$m-6$	$m-4$	$m-2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$m-3$	0	$m-3$	$m-6$	$\dots$	12	6	3
$m-2$	0	$m-2$	$m-4$	$\dots$	6	4	2
$m-1$	0	$m-1$	$m-2$	$\dots$	3	2	1

§ 17.5.6 Grupo de permutaciones. Grupo simétrico

Teorema 17.29 (Grupo de permutaciones de un conjunto)
Sea X un conjunto no vacío, P_X el conjunto de todas las biyecciones de X en X y $\circ$ la operación composición de aplicaciones. Entonces, $(P_X, \circ)$ tiene estructura de grupo no conmutativo. Lo llamamos *grupo de permutaciones de* X.

Definición 17.37.— Si $\exists n \in \mathbb{Z}^+, X = [n]^+$, entonces llamamos a P_X *grupo simétrico de orden* n o *grupo de las permutaciones de orden* $\boldsymbol{n}$ o *grupo de las sustituciones de orden* $\boldsymbol{n}$ y lo notamos S_n.

Observación 17.5.6.— En el caso finito, una k-permutación (o k-sustitución) ordinaria de n objetos no es más que una disposición ordenada de k objetos de los n. Caso de considerar un conjunto ordenado de objetos y ser $k = n$, se trata de una reordenación del conjunto.

Teorema 17.30

El número de permutaciones de un conjunto de n elementos es el producto $n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$ (que se abrevia por $n!$ —«n factorial»—). Dicho número es el mismo que el número de diferentes ordenaciones existentes de esos n elementos. Lo designamos por P_n.

Teorema 17.31

Precisamente P_n es el número total de aplicaciones biyectivas entre dos conjuntos de n elementos.

Representamos la permutación $\sigma \in S_n$ por la disposición matricial

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Permutaciones y programación lineal entera

Hemos tenido oportunidad de aprender ya que, dependiendo del contexto y del interés computacional, la representación del conocimiento es diversa. En el caso de las permutaciones, observemos una representación alternativa, de interés en programación lineal entera*: por ejemplo, si las filas corresponden por orden a las entidades a, b y c, y las columnas, también por orden, a las posiciones en la permutación, entonces la matriz

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

representa la permutación c, a, b.

* *Cfr. v. gr.* PARDO, FELIPE y PARDO [192] (pág. 55).

Ejemplo 455

S_3, el grupo de las permutaciones de $A = \{1, 2, 3\}$, tiene 6 elementos.

Resolución.— En efecto, las $3! = 6$ permutaciones de tres elementos —biyecciones de $\{1, 2, 3\}$ a $\{1, 2, 3\}$— son:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$ ■

Ejemplo 456

Demostremos que τ_2 y τ_3 conforman un ejemplo de que $\circ$ no satisface la conmutativa en S_3.

Resolución.— En efecto,

$$\tau_3 \circ \tau_2 = \tau_3(\tau_2) = \tau_3 \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_2;$$

$$\tau_2 \circ \tau_3 = \tau_2(\tau_3) = \tau_2 \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_1.$$ ■

Teorema 17.32
Sea $\sigma \in S_n$. La relación diádica E_σ definida por $(\forall x, y \in [n]^+)(xE_\sigma y \leftrightarrow (\exists n \in \mathbb{Z})(y = \sigma^n(x)))$ es una relación de equivalencia en $[n]^+$.

Definición 17.38.— Dados $x \in [n]^+$, $\sigma \in S_n$ y la equivalencia E_σ, se denomina *órbita* de x respecto de σ, y se nota $\text{orb}_\sigma(x)$, a la clase de equivalencia a la que pertenece x.

Teorema 17.33
Dados $x \in [n]^+$ y $\sigma \in S_n$, $\text{orb}_\sigma(x) = \{\sigma(x), \sigma^2(x), \ldots, \sigma^t(x)\}$, donde t es el menor entero positivo tal que $\sigma^t(x) = x$.

Ejemplo 457

Hallemos las órbitas de la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 6 & 1 & 3 & 8 & 2 & 5 & 7 & 0 \end{pmatrix}.$$

Resolución.— Las órbitas son:

$$\text{orb}_\sigma(0) = \{\sigma(0), \sigma^2(0)\} = \{9, 0\}$$

$$\text{orb}_\sigma(1) = \{\sigma(1), \sigma^2(1), \sigma^3(1)\} = \{4, 3, 1\}$$

$$\text{orb}_\sigma(2) = \{\sigma(2), \sigma^2(2)\} = \{6, 2\}$$

$$\text{orb}_\sigma(3) = \{\sigma(3), \sigma^2(3), \sigma^3(3)\} = \{1, 4, 3\}$$

$$\text{orb}_\sigma(4) = \{\sigma(4), \sigma^2(4), \sigma^3(4)\} = \{3, 1, 4\}$$

$$\mathrm{orb}_\sigma(5) = \{\sigma(5), \sigma^2(5), \sigma^3(5)\} = \{8, 7, 5\}$$

$$\mathrm{orb}_\sigma(6) = \{\sigma(6), \sigma^2(6)\} = \{2, 6\}$$

$$\mathrm{orb}_\sigma(7) = \{\sigma(7), \sigma^2(7), \sigma^3(7)\} = \{5, 8, 7\}$$

$$\mathrm{orb}_\sigma(8) = \{\sigma(8), \sigma^2(8), \sigma^3(8)\} = \{7, 5, 8\}$$

$$\mathrm{orb}_\sigma(9) = \{\sigma(9), \sigma^2(9)\} = \{0, 9\}$$

■

Ciclos

Definición 17.39.— Sea $\sigma \in S_n$. Decimos que σ es un *ciclo* de longitud k (o k-ciclo) precisamente si σ intercambia cíclicamente k elementos, manteniendo fijos el resto. Esto es, precisamente si existen $a_1, a_2, \ldots, a_k \in [n]^+$ tales que:

$$\sigma(x) = \begin{cases} a_{i+1} & \text{si} \quad x = a_i \wedge i \in [k-1]^+ \\ a_1 & \text{si} \quad x = a_k \\ x & \text{si} \quad x \neq a_i \wedge i \in [k]^+ \end{cases}$$

Notamos un ciclo por $(a_1\ a_2\ \ldots\ a_k)$, indicando que $\sigma\,(a_h) = a_{h+1}$.

Definición 17.40.— Si $k = n$, decimos que σ es una *permutación cíclica* (o, sinónimamente, *permutación circular*).

Ejemplo 458

Representemos las permutaciones de S_3 como ciclos.

Resolución.— Las permutaciones de S_3 son:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = 1, \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3), \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2),$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3), \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3), \qquad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2).$$

■

Ejemplo 459

¿Cuáles son las 7 permutaciones cíclicas de la palabra binaria 1100010?

Resolución.— Éstas: 1100010, 0110001, 1011000, 0101100, 0010110, 0001011 y 1000101. ■

Teorema 17.34

Sea $\gamma = (a_1\ a_2\ \ldots\ a_k) \in S_n$ un ciclo de longitud k. Entonces:

0. $a_i = \gamma^{i-1}(a_1)$;
1. $o(\gamma) = k$ (el orden de γ es k);
2. $\mathrm{orb}_\gamma(x) = \begin{cases} \{a_1, a_2, \ldots, a_k\} & \text{si} \quad x = a_i \land i \in [k]^+ \\ \{x\} & \text{si} \quad x \neq a_i \land i \in [k]^+ \end{cases}$;
3. $\forall x \in \{a_1, a_2, \ldots, a_k\}, \gamma = (\gamma(x)\ \gamma^2(x)\ \ldots\ \gamma^k(x))$.

Observación 17.5.7.— 0. Sea $\gamma = (a_1\ a_2\ \ldots\ a_k) \in S_n$ un ciclo de longitud k. El conjunto cociente de la relación de equivalencia E_γ asociada a γ consta de $n-k+1$ clases de equivalencia, una de cardinal k y el resto unitarias —el total de clases del tipo $\mathrm{orb}_\gamma(x) = \{x\}$, con $x \in S_n, x \neq a_i, i \in [k]^+$—.

1. Es posible expresar un ciclo de longitud k de k formas distintas. Por ejemplo, es posible expresar el ciclo $(1\ 2\ 3)$ de tres formas, a saber: $(1\ 2\ 3)$, $(2\ 3\ 1)$ y $(3\ 1\ 2)$.

Definición 17.41.— Decimos que $\gamma = (a_1\ a_2\ \ldots\ a_k) \in S_n$ y $\tau = (b_1\ b_2\ \ldots\ b_l) \in S_n$ son *ciclos disjuntos*, precisamente si sus órbitas no unitarias son disjuntas, es decir, si, y sólo si, $\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_l\} = \emptyset$.

Teorema 17.35

Dos ciclos disjuntos cualesquiera, conmutan. Esto es, si $\gamma \in S_n$ y $\tau \in S_n$ son dos ciclos disjuntos, entonces $(\forall x \in [n]^+)(\gamma\tau(x) = \tau\gamma(x))$.

Teorema 17.36 (Factorización de una permutación)

Toda permutación $\sigma \in S_n$, $\sigma \neq 1$ y no ciclo, se puede expresar de forma única, salvo el orden de los factores, como producto de ciclos disjuntos. Concretamente, siendo $\sigma \in S_n$, $\sigma \neq 1$ y no ciclo, entonces:

0. sea $x \in [n]^+$ tal que $\sigma(x) \neq x$ y $\mathrm{orb}_\sigma(x) = \{\sigma(x), \sigma^2(x), \ldots, \sigma^t(x)\}$ —con $t > 1$, ya que la órbita no es unitaria—, entonces, si asociamos a dicha órbita el ciclo $\gamma = (\sigma(x)\ \sigma^2(x)\ \ldots\ \sigma^t(x))$, se tiene que $\mathrm{orb}_\sigma(x) = \mathrm{orb}_\gamma(x)$;
1. si $\mathrm{orb}_\sigma(a_{i_1}), \mathrm{orb}_\sigma(a_{i_2}), \ldots, \mathrm{orb}_\sigma(a_{i_l})$ son las distintas órbitas no unitarias y $\gamma_1, \gamma_2, \ldots, \gamma_l$ sus ciclos asociados, entonces $\sigma = \gamma_1\gamma_2\cdots\gamma_l$.

Ejemplo 460

Escribamos la siguiente permutación σ como producto de ciclos disjuntos:

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 6 & 1 & 3 & 8 & 2 & 5 & 7 & 0 \end{pmatrix}.$$

Resolución.— Consideremos las órbitas disjuntas $\mathrm{orb}_\sigma(i)$:

$\mathrm{orb}_\sigma(1) = \{\sigma(1), \sigma^2(1), \sigma^3(1)\} = \{4, 3, 1\}$;

$\mathrm{orb}_\sigma(2) = \{\sigma(2), \sigma^2(2)\} = \{6, 2\}$;

$\mathrm{orb}_\sigma(5) = \{\sigma(5), \sigma^2(5), \sigma^3(5)\} = \{8, 7, 5\}$;

$\mathrm{orb}_\sigma(9) = \{\sigma(9), \sigma^2(9)\} = \{0, 9\}$.

Consideremos los siguientes ciclos, asociados a estas órbitas:

$\gamma_1 = (\sigma(1)\ \sigma^2(1)\ \sigma^3(1)) = (4\ 3\ 1)$;

$\gamma_2 = (\sigma(2)\ \sigma^2(2)) = (6\ 2)$;

$\gamma_5 = (\sigma(5)\ \sigma^2(5)\ \sigma^3(5)) = (8\ 7\ 5)$;

$\gamma_9 = (\sigma(9)\ \sigma^2(9)) = (0\ 9)$.

Por el teorema anterior,

$$\sigma = \gamma_1\gamma_2\gamma_5\gamma_9,$$

es decir,

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 6 & 1 & 3 & 8 & 2 & 5 & 7 & 0 \end{pmatrix} = (4\ 3\ 1)(6\ 2)(8\ 7\ 5)(0\ 9).$$



Teorema 17.37

Un método práctico para escribir una permutación como producto de ciclos disjuntos es el siguiente:

0.º, El primer elemento del primer ciclo es cualquier elemento; el segundo es la imagen del primero; el tercero, la del segundo. . ., y así sucesivamente, hasta que el primero sea la imagen del último. Decimos que se ha completado un ciclo.

1.º, El primer elemento del segundo ciclo es cualquier elemento que no aparezca en el primer ciclo; el segundo, la imagen del primero, el tercero, la del segundo, así hasta que el primero sea la imagen del último.

2.º, Repetimos este proceso hasta que todos los elementos aparezcan en algún ciclo. Pudiésemos no considerar los ciclos unitarios, puesto que se corresponden con la permutación identidad.

Ejemplo 461

Siguiendo este método, escribamos la permutación σ del último ejemplo como producto de ciclos disjuntos.

Resolución.— Según este método y además siguiendo un recorrido secuencial de búsqueda de elementos que no aparezcan en ciclos anteriores,

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 6 & 1 & 3 & 8 & 2 & 5 & 7 & 0 \end{pmatrix} = (0\ 9)(1\ 4\ 3)(2\ 6)(5\ 8\ 7). \qquad \blacksquare$$

Ejemplo 462

Sea $\sigma : [2n]^+ \to [2n]^+$ definida por $\sigma(n) = n + (-1)^{n+1}$. Escribámosla como producto de ciclos disjuntos.

Resolución.— Según su definición, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & 2n-1 & 2n \\ 2 & 1 & 4 & 3 & \cdots & 2n & 2n-1 \end{pmatrix}$. Y como producto de ciclos disjuntos, siguiendo el método expuesto:

$$\sigma = (1\ 2)(3\ 4)\cdots(2n-1\ 2n). \qquad \blacksquare$$

Teorema 17.38

Si $\sigma \in S_n$ es un producto de ciclos disjuntos, entonces su orden es el mínimo común múltiplo de los órdenes de los ciclos.

Transposiciones

Definición 17.42.— Llamamos *transposición* a todo ciclo de longitud 2. Notamos por $(i\ j)$, indicando que los elementos i y j son los que se intercambian, permaneciendo el resto igual.

Teorema 17.39

Todo ciclo de longitud k puede ser expresado como producto de $k-1$ transposiciones, por ejemplo, así: $(a_1\ a_2\ \dots\ a_k) = (a_k\ a_1)(a_{k-1}\ a_1)\dots(a_2\ a_1)$.

Teorema 17.40

0. Es posible escribir toda permutación, de forma no única, como producto de transposiciones.
1. *Invarianza de la paridad*: Dada una permutación, el número de transposiciones necesario para escribirla es par o impar, dependiendo únicamente de la permutación y no de las transposiciones intervinientes.

Ejemplo 463

Expresemos las permutaciones de S_3 como producto de transposiciones.

Resolución.— Para conseguirlo, vamos a partir de su representación como ciclos (*vid. supra* ejemplo 17.5.6 (pág. 873 de esta edición) y a utilizar la estrategia mencionada en el teorema 17.39 (pág. 877 de esta edición):

$$\mathrm{id} = 1, \qquad \sigma_1 = (1\ 2\ 3) = (3\ 1)(2\ 1), \qquad \sigma_2 = (1\ 3\ 2) = (2\ 1)(3\ 1),$$
$$\tau_1 = (2\ 3), \qquad \tau_2 = (1\ 3), \qquad \tau_3 = (1\ 2).$$

■

Observación 17.5.8.— En la resolución del ejemplo anterior apreciamos que hay tres permutaciones pares y tres impares (id es par porque se necesitan cero transposiciones para escribirla). Esto es un resultado general, siempre sucede que la mitad de las permutaciones son pares y la otra mitad, impares.

Observación 17.5.9.— La representación no es única. En el ejemplo anterior, además de las proporcionadas por el teorema 17.39 (pág. 877 de esta edición), tenemos, por ejemplo: $\sigma_1 = (1\ 2)(2\ 3)$ y $\sigma_2 = (1\ 2)(1\ 3) = (1\ 2)(2\ 1)(1\ 2)(1\ 3)$.

Observación 17.5.10.— De la observación anterior, notemos que si los ciclos son disjuntos aseguramos la conmutatividad del producto de éstos —*cfr. supra* ejemplos 460 y 461 (págs. 875 y 876 de esta edición)—.

Signatura de una permutación

Definición 17.43.— Llamamos *signatura de una permutación* $\sigma \in S_n$, y designamos por $\varepsilon(\sigma)$, al signo de la paridad correspondiente al número de transposiciones necesario para escribirla ($+1$ si par y -1 si impar).

Definición 17.44.— Sea $\sigma \in S_n$. Decimos que $\{i, j\} \subseteq [n]^+$ es una *inversión* para σ si se satisface que $\dfrac{\sigma(i) - \sigma(j)}{i - j} < 0$. El *número de inversiones* para $\sigma \in S_n$ lo notamos por ν_σ.

Teorema 17.41
Sea $\sigma \in S_n$. La signatura de σ es el signo correspondiente a la paridad del número de inversiones de la misma, es decir, $\varepsilon(\sigma) = (-1)^{\nu_\sigma}$.

Ejemplo 464

Hallemos la signatura de

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

Resolución.— De los pares ordenados posibles,

$$(1,2), (1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5), (4,5),$$

presentan inversión los pares

$$(1,3), (1,5), (2,3), (2,5), (4,5),$$

luego,

$$\varepsilon(\sigma) = (-1)^5 = -1.$$

■

Ejemplo 465

¿Cuáles son las signaturas de las permutaciones de cuatro elementos?

Resolución.—

Permutación, σ	N. inversiones, ν_σ	Paridad	Signatura, $\varepsilon(\sigma)$
1234	0	par	$+1$
1243	1	impar	-1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
4321	6	par	$+1$

■

Teorema 17.42

La signatura de una transposición es -1.

Teorema 17.43

La signatura de un producto de permutaciones es igual al producto de signaturas.

Teorema 17.44

Si $\sigma \in S_n$ es un ciclo de longitud k, $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}$, entonces $\varepsilon(\sigma) = (-1)^{k-1}$, ya que todo ciclo de longitud k se puede expresar como producto de $k-1$ transposiciones (*vid. supra* teorema 17.39 [pág. 877]).

Ejemplo 466

Hallemos, según este último resultado, la signatura de la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 5 & 6 & 9 & 7 & 2 & 8 & 1 & 11 & 10 \end{pmatrix}.$$

Resolución.— Expresada como producto de ciclos disjuntos:

$$\sigma = (1\ 3\ 5\ 9)(2\ 4\ 6\ 7)(10\ 11).$$

Su signatura es el producto de las tres signaturas:

$$\varepsilon(\sigma) = (-1)(-1)(-1) = -1.$$

■

§ 17.6 Inicio de la lista de grupos finitos

§ 17.6.0 Orden 1

Sólo existe un grupo de orden 1 salvo isomorfismos, cuya tabla de composición es

	e
e	e

Este grupo es abeliano —observamos que la tabla es simétrica respecto de la diagonal principal— y cíclico, pues sus elementos son e, $e^2 = e$. Se conoce como el *grupo cíclico* C_1.

El grupo C_1 no tiene subgrupos propios.

Ejemplo 467

Los grupos $(\mathbb{Z}_1; +_1)$ y $\mathrm{Sim}\{X\}$, con $|X| = 1$ son modelos para C_1.

[Cubit 95].

Resolución.— En efecto,

0. un modelo para C_1 es $(\mathbb{Z}_1; +_1)$, cuyo elemento es $0 +_1 0 = 0$ y cuya tabla de composición es

$+_1$	0
0	0

;

1. otro ejemplo de modelo para C_1 es $\mathrm{Sim}\{X\}$, con $X = \{x\}$, el grupo simétrico de X —en particular, S_1—, siendo la permutación la identidad, id; la tabla de composición de $\mathrm{Sim}\{X\}$ es

$\circ$	id
id	id



§ 17.6.1 Orden 2

Sólo existe un grupo de orden 2 salvo isomorfismos, cuya tabla de composición es

	e	a
e	e	a
a	a	e

Observación 17.6.0.— Si ocurriese que $a^2 = a$, entonces a no tendría simétrico, por lo que necesariamente $a^2 = e$.

Este grupo es abeliano —observamos que la tabla es simétrica respecto de la diagonal principal— y cíclico, pues sus elementos son a, $a^2 = e$. Se conoce como el *grupo cíclico* C_2.

El grupo C_2 no tiene subgrupos propios.

Ejemplo 468

Los grupos $(\mathbb{Z}_2; +_2)$ y $\mathrm{Sim}\{X\}$, con $|X| = 2$ son modelos para C_2.

[Cubit 96].

Resolución.— En efecto,

0. un modelo para C_2 es $(\mathbb{Z}_2; +_2)$, cuyos elementos son $1, 1 +_2 1 = 0$ y cuya tabla de composición es

$+_2$	0	1
0	0	1
1	1	0

;

1. otro ejemplo de modelo para C_2 es $\mathrm{Sim}\{X\}$, con $X = \{x, y\}$, el grupo simétrico de X —en particular, S_2—, siendo las dos permutaciones, notémoslas, σ_0, $\sigma_0 \circ \sigma_0 = \mathrm{id}$; la tabla de composición de $\mathrm{Sim}\{X\}$ es

$\circ$	id	σ_0
id	id	σ_0
σ_0	σ_0	id

donde $\sigma_0 = \begin{pmatrix} x & y \\ y & x \end{pmatrix}$. ■

Actividad 17.3

Demostremos que $(0, 1; \veebar)$ y $(0, 1; \leftrightarrow)$ son modelos para C_2.

[Cubit 97].

§ 17.6.2 Orden 3

Sólo existe un grupo de orden 3 salvo isomorfismos, cuya tabla de composición es

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Este grupo es abeliano —observamos que la tabla es simétrica respecto de la diagonal principal— y cíclico, pues sus elementos son a, $a^2 = b$, $a^3 = e$. Se conoce como el *grupo cíclico* C_3.

El grupo C_3 no tiene subgrupos propios.

Ejemplo 469

El grupo $(\mathbb{Z}_3; +_3)$ es un modelo para C_3.

[Cubit 98].

Resolución.— En efecto, un modelo para C_3 es $(\mathbb{Z}_3; +_3)$, cuyos elementos son $1, 1 +_3 1 = 2, 1 +_3 1 +_3 1 = 0$ y cuya tabla es

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

■

Observación 17.6.1.— Pudiésemos presentar un grupo de múltiples formas, por ejemplo, con mosaicos de colores[10].

Actividad 17.4

Demostremos que otro ejemplo de modelo para C_3 es el grupo de las isometrías que dejan invariante[11]el trisquel —trípode con los segmentos acodados en ángulo recto y sentido levógiro— en el plano euclideo.

[Cubit 99].

Observación 17.6.2.— Una vez hecha la actividad anterior, podremos comprobar que la tabla de composición de dicho grupo es la subtabla correspondiente a $\{\mathrm{id}, \sigma_1, \sigma_2\}$ de la tabla de composición de S_3.[12]

§ 17.6.3 Orden 4

Sólo existen dos grupos de orden 4 no isomorfos,

- el grupo cíclico C_4,
- el grupo de Klein K_4 —grupo cuadrático o del rectángulo, también denotado V_4 (*Vierergrupe* de Klein)—.

[10] *Vid. v. gr.* https://mathworld.wolfram.com/CyclicGroupC3.html

[11] El concepto de invarianza quizás nos sea ya conocido. Un *invariante de una curva* es una expresión que no varía al realizar rotaciones y traslaciones paralelas de los ejes de coordenadas. Por ejemplo, de la curva de segundo orden $a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_1x + 2a_2y + a = 0$ son invariantes: $s = a_{11} + a_{22}$ (la suma de los coeficientes de los términos cuadráticos); $\delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix}$ (el determinante de los coeficientes de los términos no lineales), y el determinante de todos los coeficientes $\Delta = \begin{vmatrix} a_{11} & a_{12} & a_1 \\ a_{12} & a_{22} & a_2 \\ a_1 & a_2 & a \end{vmatrix}$.

[12] *Vid. infra* § 17.6.5 (pág. 887 de esta edición).

El grupo cíclico C_4

La tabla de composición del *grupo cíclico* C_4 es

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Este grupo es abeliano —observamos que la tabla es simétrica respecto de la diagonal principal— y cíclico, pues sus elementos son a, $a^2 = b$, $a^3 = c$, $a^4 = e$.

El único subgrupo propio de C_4 es el de conjunto soporte $\{e, b\}$, isomorfo a C_2. El diagrama de HASSE del retículo de los subgrupos de C_4 es

$$\{e, a, b, c\}$$
$$|$$
$$\{e, b\}$$
$$|$$
$$\{e\}$$

Ejemplo 470

El grupo $(\mathbb{Z}_4; +_4)$ es un modelo para C_4.

[Cubit 100].

Resolución.— En efecto, un modelo para C_4 es $(\mathbb{Z}_4; +_4)$, cuyos elementos son $1, 1 +_4 1 = 2, 1 +_4 1 +_4 1 = 3, 1 +_4 1 +_4 1 +_4 1 = 0$ y cuya tabla de composición es

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2



Observación 17.6.3.— Otro modelo para C_4 es el grupo que hemos estudiado en el ejemplo 454 (pág. 867 de esta edición).

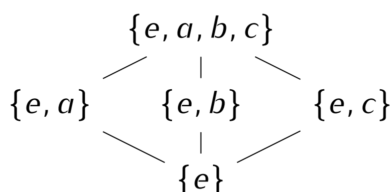
El grupo de Klein K_4

La tabla de composición de *grupo* K_4 es

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

que no es cíclico, aunque sí abeliano.

Los subgrupos propios de K_4 son los de conjuntos soporte $\{e, a\}$, $\{e, b\}$ y $\{e, c\}$, todos isomorfos a C_2. El diagrama de Hasse del retículo de los subgrupos de K_4 es



Definición 17.45.— El producto directo de dos magmas $(G; *)$ y $(H; \circ)$ es el magma $(G \times H; \cdot)$, donde $\cdot$ se define, $\forall \langle g_0, h_0\rangle, \langle g_1, h_1\rangle \in G \times H$, por $\langle g_0, h_0\rangle \cdot \langle g_1, h_1\rangle = \langle g_0 * g_1, h_0 \circ h_1\rangle$.

Teorema 17.45

El producto directo $C_2 \times C_2$ es isomorfo a K_4; su tabla de composición es

	$\langle e, e\rangle$	$\langle e, a\rangle$	$\langle a, e\rangle$	$\langle a, a\rangle$
$\langle e, e\rangle$	$\langle e, e\rangle$	$\langle e, a\rangle$	$\langle a, e\rangle$	$\langle a, a\rangle$
$\langle e, a\rangle$	$\langle e, a\rangle$	$\langle e, e\rangle$	$\langle a, a\rangle$	$\langle a, e\rangle$
$\langle a, e\rangle$	$\langle a, e\rangle$	$\langle a, a\rangle$	$\langle e, e\rangle$	$\langle e, a\rangle$
$\langle a, a\rangle$	$\langle a, a\rangle$	$\langle a, e\rangle$	$\langle e, a\rangle$	$\langle e, e\rangle$

Ejemplo 471

El grupo $(\mathbb{Z}_2 \times \mathbb{Z}_2; +_{2,2})$ es un modelo para K_4.

[Cubit 101].

Resolución.— Se sigue del teorema anterior. ■

Teorema 17.46 (Teorema de CAYLEY)
Todo grupo G es isomorfo a un subgrupo de su grupo de permutaciones S_G (aplicaciones biyectivas de G en G y la operación $\circ$). Si $|G| = n$, entonces G es isomorfo a un subgrupo de S_n.

Observación 17.6.4.— Un subgrupo de S_{48} destacado por su popularidad es el del cubo de Rubik[13].

Actividad 17.5

Demostremos que otro ejemplo de modelo para K_4 es el grupo de las isometrías que dejan invariante el rectángulo no cuadrado en el plano euclideo.

[Cubit 102].

Ejemplo 472

El grupo de KLEIN K_4 es isomorfo a un subgrupo del grupo de permutaciones S_4 de un conjunto de 4 elementos.

Resolución.— K_4 es isomorfo a $(P; \circ)$, subgrupo de S_4, con $P = \{p_{\mathrm{id}}, p_a, p_b, p_c\}$ y $p_{\mathrm{id}} = (1)$, $p_a = (1\,2)\,(3\,4)$, $p_b = (1\,3)\,(2\,4)$, $p_c = (1\,4)\,(2\,3)$. ■

§ 17.6.4 Orden 5

Sólo existe un grupo de orden 5 salvo isomorfismos, cuya tabla de composición es

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Este grupo es abeliano —observamos que la tabla es simétrica respecto de la diagonal principal— y cíclico, pues sus elementos son a, $a^2 = b$, $a^3 = c$, $a^4 = d$, $a^5 = e$. Se conoce como el *grupo cíclico* C_5.

El grupo C_5 no tiene subgrupos propios.

[13] *Vid. v. gr.* https://es.wikipedia.org/wiki/Grupo_del_cubo_de_Rubik.

Ejemplo 473

El grupo $(\mathbb{Z}_5; +_5)$ es un modelo para C_5.

[Cubit 103].

Resolución.— En efecto, un modelo para C_5 es $(\mathbb{Z}_5; +_5)$, cuyos elementos son $1, 1 +_5 1 = 2, 1 +_5 1 +_5 1 = 3, 1 +_5 1 +_5 1 +_5 1 = 4, 1 +_5 1 +_5 1 +_5 1 +_5 1 = 0$ y cuya tabla de composición es

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

■

§ 17.6.5 Orden 6

Sólo existen dos grupos de orden 6 no isomorfos,

- el grupo cíclico C_6, abeliano,
- el grupo simétrico S_3, no abeliano.

Observación 17.6.5.— En este acercamiento elemental a los grupos finitos prefiero destacar a S_3 y no al producto semidirecto $C_3 \rtimes C_2$ del cual, en realidad, es un modelo.

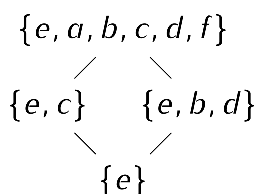
El grupo cíclico C_6

La tabla de composición del *grupo cíclico* C_6 es

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

que, en efecto, es cíclico, pues sus elementos son a, $a^2 = b$, $a^3 = c$, $a^4 = d$, $a^5 = f$, $a^6 = e$. C_6 es un grupo abeliano —observamos que su tabla es simétrica—.

Los subgrupos propios de C_6 son los de conjunto soporte $\{e, c\}$ —isomorfo a C_2— y $\{e, b, d\}$ —isomorfo a C_3—. El diagrama de Hasse del retículo de los subgrupos de C_6 es



Ejemplo 474

El grupo $(\mathbb{Z}_6; +_6)$ es un modelo para C_6.

[Cubit 104].

Resolución.— En efecto, un modelo para C_6 es $(\mathbb{Z}_6; +_6)$, cuyos elementos son $1, 1+_6 1 = 2, 1+_6 1+_6 1 = 3, 1+_6 1+_6 1+_6 1 = 4, 1+_6 1+_6 1+_6 1+_6 1 = 5, 1+_6 1+_6 1+_6 1+_6 1+_6 1 = 0$ y cuya tabla de composición es

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

■

El grupo simétrico S_3

El *grupo simétrico* S_3 de las permutaciones de tres elementos no es abeliano ni cíclico; su tabla de composición es

$\circ$	id	σ_1	σ_2	τ_1	τ_2	τ_3
id	id	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	id	τ_3	τ_1	τ_2
σ_2	σ_2	id	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	id	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	id	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	id

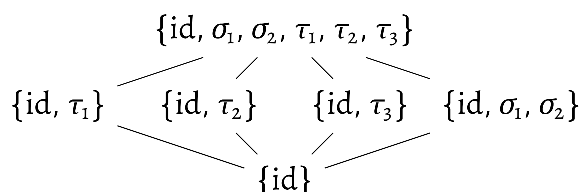
donde, como vimos en el ejemplo 455 (pág. 871 de esta edición), las $3! = 6$ permutaciones de 3 elementos —biyecciones de $\{1, 2, 3\}$ a $\{1, 2, 3\}$— son:

$$\text{id} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Como hemos dicho, S_3 no es abeliano[14]. De hecho, S_3 es el grupo no abeliano más pequeño.

Los subgrupos propios de S_3 son los de conjunto soporte $\{id, \tau_1\}$, $\{id, \tau_2\}$ y $\{id, \tau_3\}$ —todos isomorfos a C_2— y $\{id, \sigma_1, \sigma_2\}$ —isomorfo a C_3—. El diagrama de Hasse del retículo de los subgrupos de S_3 es



Para $n \geq 3$, el grupo S_n no es abeliano.

Observación 17.6.6.— Vemos una presentación de S_3 que destaca el hecho de ser mutuamente simétricos σ_1 y σ_2, en el artículo correspondiente de la Wikipedia en francés[15] .

Ejemplo 475

El *grupo diédrico* D_3 de las isometrías que dejan invariante el triángulo equilátero en el plano euclideo (también es conocido como el *grupo del triángulo*) es isomorfo a S_3.

[Cubit 105].

Resolución.— Dichas isometrías son las rotaciones de 120° ($2\pi/3$ rad), 240° ($4\pi/3$ rad) y 360° ($6\pi/3$ rad), que abreviaremos, respectivamente, por r, r^{-1} (es la inversa de r) e id (la rotación de 360° es la identidad), y simetrías axiales (reflexiones) de ejes las mediatrices de ángulos de inclinación 30° ($\pi/6$ rad), 150° ($5\pi/6$ rad) y 270° ($9\pi/6$ rad), que abreviaremos, respectivamente, por s_1, s_2 y s_0.

$\circ$	id	r	r^{-1}	s_0	s_1	s_2
id	id	r	r^{-1}	s_0	s_1	s_2
r	r	r^{-1}	id	s_2	s_0	s_1
r^{-1}	r^{-1}	id	r	s_1	s_2	s_0
s_0	s_0	s_1	s_2	id	r	r^{-1}
s_1	s_1	s_2	s_0	r^{-1}	id	r
s_2	s_2	s_0	s_1	r	r^{-1}	id

[14] *Cfr. supra* ejemplo 456 (pág. 872 de esta edición).
[15] *Vid.* https://fr.wikipedia.org/wiki/Groupe_symétrique.

La comparación de sus tablas de composición nos permite comprobar que D_3 es isomorfo a S_3; la biyección es: $\mathrm{id} \longleftrightarrow \mathrm{id}$, $\sigma_1 \longleftrightarrow r$, $\sigma_2 \longleftrightarrow r^{-1}$, $\tau_1 \longleftrightarrow s_0$, $\tau_2 \longleftrightarrow s_1$, $\tau_3 \longleftrightarrow s_2$. ■

Observación 17.6.7.— Vemos otras presentaciones de D_3 en el artículo correspondiente de Proof Wiki[16].

§ 17.6.6 Orden 7

Sólo existe un grupo de orden 7 salvo isomorfismos, el *grupo cíclico* C_7, que no tiene subgrupos propios.

§ 17.6.7 Orden 8

Existen cinco grupos de orden 8 no isomorfos, tres son abelianos,

- el grupo cíclico C_8 —que tiene dos subgrupos propios, isomorfos a C_2 y C_4—,
- el grupo producto directo $C_2 \times C_4$ —que tiene seis subgrupos propios: tres isomorfos a C_2, dos a C_4 y uno a K_4—,
- el grupo producto directo $C_2 \times C_2 \times C_2$ —que tiene catorce subgrupos propios: siete isomorfos a C_2 y siete isomorfos a K_4—,

y dos son no abelianos,

- el grupo diédrico D_4 —que tiene siete subgrupos propios: cinco isomorfos a C_2, uno isomorfo a C_4 y dos isomorfos a K_4—,
- el grupo Q_8 de cuaterniones[17] —que tiene cuatro subgrupos propios: uno isomorfo a C_2 y tres isomorfos a C_4—.

El grupo diédrico D_4

El *grupo diédrico* D_4 es el de las isometrías que dejan invariante el cuadrado en el plano euclideo. Se le conoce como *grupo del cuadrado*.[18]

[Cubit 106].

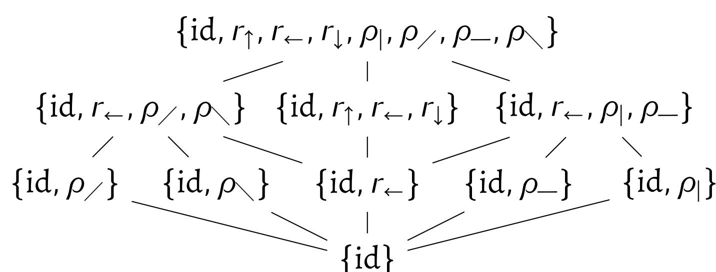
Dichas isometrías son las rotaciones de 90° ($\pi/2$ rad), 180° ($2\pi/2$ rad), 270° ($3\pi/2$ rad) y 360° ($4\pi/2$ rad), que abreviaremos, respectivamente, por $r_\uparrow$, $r_\leftarrow$, $r_\downarrow$ e id (la rotación de 360° es la identidad),

[16] *Vid.* https://proofwiki.org/wiki/Definition:Dihedral_Group_D3.
[17] *Vid. v. gr.* https://en.wikipedia.org/wiki/Quaternion.
[18] *Vid. v. gr.* https://en.wikipedia.org/wiki/Dihedral_group y https://en.wikipedia.org/wiki/Dihedral_group_of_order_8.

y simetrías axiales (reflexiones) de ejes OX, OY y las diagonales, que notaremos ρ_{-}, $\rho_{|}$, $\rho_{\diagup}$ y $\rho_{\diagdown}$ respectivamente.

$\circ$	id	$r_{\uparrow}$	$r_{\leftarrow}$	$r_{\downarrow}$	$\rho_{|}$	$\rho_{\diagup}$	ρ_{-}	$\rho_{\diagdown}$
id	id	$r_{\uparrow}$	$r_{\leftarrow}$	$r_{\downarrow}$	$\rho_{|}$	$\rho_{\diagup}$	ρ_{-}	$\rho_{\diagdown}$
$r_{\uparrow}$	$r_{\uparrow}$	$r_{\leftarrow}$	$r_{\downarrow}$	id	$\rho_{\diagdown}$	$\rho_{|}$	$\rho_{\diagup}$	ρ_{-}
$r_{\leftarrow}$	$r_{\leftarrow}$	$r_{\downarrow}$	id	$r_{\uparrow}$	ρ_{-}	$\rho_{\diagdown}$	$\rho_{|}$	$\rho_{\diagup}$
$r_{\downarrow}$	$r_{\downarrow}$	id	$r_{\uparrow}$	$r_{\leftarrow}$	$\rho_{\diagup}$	ρ_{-}	$\rho_{\diagdown}$	$\rho_{|}$
$\rho_{|}$	$\rho_{|}$	$\rho_{\diagup}$	ρ_{-}	$\rho_{\diagdown}$	id	$r_{\uparrow}$	$r_{\leftarrow}$	$r_{\downarrow}$
$\rho_{\diagup}$	$\rho_{\diagup}$	ρ_{-}	$\rho_{\diagdown}$	$\rho_{|}$	$r_{\downarrow}$	id	$r_{\uparrow}$	$r_{\leftarrow}$
ρ_{-}	ρ_{-}	$\rho_{\diagdown}$	$\rho_{|}$	$\rho_{\diagup}$	$r_{\leftarrow}$	$r_{\downarrow}$	id	$r_{\uparrow}$
$\rho_{\diagdown}$	$\rho_{\diagdown}$	$\rho_{|}$	$\rho_{\diagup}$	ρ_{-}	$r_{\uparrow}$	$r_{\leftarrow}$	$r_{\downarrow}$	id

Los subgrupos propios de D_4 son los de conjunto soporte $\{\mathrm{id}, \rho_{\diagup}\}$, $\{\mathrm{id}, \rho_{\diagdown}\}$, $\{\mathrm{id}, r_{\leftarrow}\}$, $\{\mathrm{id}, \rho_{-}\}$ y $\{\mathrm{id}, \rho_{|}\}$ —todos isomorfos a C_2— y $\{\mathrm{id}, r_{\leftarrow}, \rho_{\diagup}, \rho_{\diagdown}\}$ —isomorfo a K_4—, $\{\mathrm{id}, r_{\uparrow}, r_{\leftarrow}, r_{\downarrow}\}$ —isomorfo a C_4— y $\{\mathrm{id}, r_{\leftarrow}, \rho_{|}, \rho_{-}\}$ —isomorfo a K_4—. El diagrama de Hasse del retículo de los subgrupos de D_4 es



El grupo diédrico D_4 es finitamente generado. Sus generadores son $r_{\uparrow}$ y $\rho_{|}$. En efecto, los elementos de D_4 son $\rho_{|} \circ \rho_{|} = \mathrm{id}$, $r_{\uparrow}$, $r_{\uparrow}^2 = r_{\leftarrow}$, $r_{\uparrow}^3 = r_{\downarrow}$, $\rho_{|}$, $\rho_{|} \circ r_{\uparrow}^2 = \rho_{-}$, $\rho_{|} \circ r_{\uparrow} = \rho_{\diagup}$, $\rho_{|} \circ r_{\uparrow}^3 = \rho_{\diagdown}$. Su tabla de composición expresada genéricamente en función de sus dos generadores renombrados respectivamente como a y b es[19]

	e	a	a^2	a^3	b	ba	ba^2	ba^3
e	e	a	a^2	a^3	b	ba	ba^2	ba^3
a	a	a^2	a^3	e	ba^3	b	ba	ba^2
a^2	a^2	a^3	e	a	ba^2	ba^3	b	ba
a^3	a^3	e	a	a^2	ba	ba^2	ba^3	b
b	b	ba	ba^2	ba^3	e	a	a^2	a^3
ba	ba	ba^2	ba^3	b	a^3	e	a	a^2
ba^2	ba^2	ba^3	b	ba	a^2	a^3	e	a
ba^3	ba^3	b	ba	ba^2	a	a^2	a^3	e

Para saber más, *vid. v. gr.* https://en.wikipedia.org/wiki/List_of_small_groups.

[19] *Cfr. v. gr.* https://proofwiki.org/wiki/Definition:Dihedral_Group_D4.

Observación 17.6.8.— Pudiésemos utilizar SageMath para consolidar nuestros conocimientos de grupos[20]. Un ejemplo ingenuo:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
# mostrando la tabla de Cayley de S3
S3 = SymmetricGroup(3)
TS3 = S3.cayley_table()
print(TS3)
# mostrando los elementos de S3
print(S3.list())
# mostrando la tabla de Cayley de D4
D4 = DihedralGroup(4)
TD4 = D4.cayley_table()
print(TD4)
```

Actividad 17.6

El *grupo diédrico* D_6 es el de las isometrías que dejan invariante el hexágono regular en el plano euclideo. Se le conoce como *grupo del hexágono*. ¿Cuáles son dichas isometrías? Hagamos su tabla de Cayley.

Con miras a su resolución.— El hexágono regular tiene seis simetrías axiales —tres con respecto a las rectas que pasan por vértices opuestos y tres con respecto a las rectas que pasan por los puntos medios de lados opuestos— y seis rotaciones —de ángulos 0, $\frac{\pi}{3}$, $\frac{2\pi}{3}$, π, $\frac{4\pi}{3}$ y $\frac{5\pi}{3}$ radianes—.

§ 17.6.8 El teorema enorme

El *teorema de clasificación de los grupos simples finitos* —grupos que no contienen subgrupos normales propios— es conocido como el *teorema enorme*.

Para saber más, *vid. v. gr.* https://en.wikipedia.org/wiki/Classification_of_finite_simple_groups.

[20] *Cfr. v. gr.* https://doc.sagemath.org/html/en/thematic_tutorials/group_theory.html.

§ 17.6.9 Muestra de ejemplos

Ejemplo 476

En el conjunto $\mathbb{Q}$ de los números racionales, consideremos la ley de composición diádica: $\forall x, y \in \mathbb{Q}, x * y = x + y - x \cdot y$, siendo $+$, $-$ y $\cdot$ la suma, la diferencia y el producto habituales en $\mathbb{Q}$.

0. Estudiemos la estructura algebraica $(\mathbb{Q}; *)$.
1. Encontremos un subconjunto propio A de Q tal que $(A; *)$ sea grupo abeliano, construyamos su tabla de CAYLEY y demostremos que $(A; *)$ es un grupo abeliano.

[PEP 10.4.2019:3], [EFE 28.6.2023:4].

Resolución.—

0. I. Es una operación (una ley de composición interna) en $\mathbb{Q}$, pues la suma y el producto habitual lo son y se trata de una suma de tres sumandos, uno de ellos un producto; por tanto, $(\mathbb{Q}; *)$ es un magma.

II. $\forall x, y \in \mathbb{Q}$, se tiene que

$$\begin{aligned} x * y &= x + y - x \cdot y && \text{[definición de } *] \\ &= y + x - x \cdot y && \text{[conmutativa de } + \text{ en } \mathbb{Q}] \\ &= y + x - y \cdot x && \text{[conmutativa de } \cdot \text{ en } \mathbb{Q}] \\ &= y * x, && \text{[definición de } *] \end{aligned}$$

por lo que $(\mathbb{Q}; *)$ es un magma abeliano (conmutativo).

III. $\forall x, y, z \in \mathbb{Q}$, se tiene, por un lado que

$$\begin{aligned} (x * y) * z &= (x + y - x \cdot y) * z && \text{[definición de } *] \\ &= x + y - x \cdot y + z - (x + y - x \cdot y) \cdot z && \text{[definición de } *] \\ &= x + y - x \cdot y + z - x \cdot z - y \cdot z + x \cdot y \cdot z, && \text{[distributiva de } \cdot \text{ en } + \text{ en } \mathbb{Q}] \end{aligned}$$

y por otro, que

$$\begin{aligned} x * (y * z) &= x * (y + z - y \cdot z) && \text{[definición de } *] \\ &= x + (y + z - y \cdot z) - x \cdot (y + z - y \cdot z) && \text{[definición de } *] \\ &= x + y + z - y \cdot z - x \cdot y - x \cdot z + x \cdot y \cdot z. && \text{[distributiva de } \cdot \text{ en } + \text{ en } \mathbb{Q}] \end{aligned}$$

De ser conmutativa $+$ en $\mathbb{Q}$ se sigue que son iguales y, por lo tanto, que $(\mathbb{Q}; *)$ es un semigrupo abeliano.

iv. El elemento neutro es el 0; por ser una estructura abeliana basta demostrarlo por un lado; por ejemplo, veamos que $\forall x \in \mathbb{Q}$, $x * 0 = x$; en efecto,

$$\begin{aligned} x * 0 &= x + 0 + x \cdot 0 && \text{[definición de } *] \\ &= (x + 0) + x \cdot 0 && \text{[asociativa de } + \text{ en } \mathbb{Q}] \\ &= x + x \cdot 0 && \text{[0 neutro de } + \text{ en } \mathbb{Q}] \\ &= x + 0 && \text{[0 absorbente de } \cdot \text{ en } \mathbb{Q}] \\ &= x && \text{[0 neutro de } + \text{ en } \mathbb{Q}] \end{aligned}$$

y, por lo tanto, $(\mathbb{Q}; *)$ es un monoide abeliano.

v. Por ser una estructura conmutativa, para encontrar el elemento simétrico de uno dado, basta buscarlo por un lado:

$$\begin{aligned} x' \text{ es el simétrico de } x &\leftrightarrow x * x' = 0 && \text{[definición de simétrico]} \\ &\leftrightarrow x + x' - x \cdot x' = 0 && \text{[definición de } *] \\ &\leftrightarrow x + (1 - x) \cdot x' = 0 && \text{[distributiva de } \cdot \text{ en } + \text{ en } \mathbb{Q}] \\ &\leftrightarrow (1 - x) \cdot x' = -x && \text{[monotonía de } + \text{ en } \mathbb{Q}] \\ &\leftrightarrow (x - 1) \cdot x' = x && \text{[monotonía de } \cdot \text{ en } \mathbb{Q}] \\ &\leftrightarrow x' = \frac{x}{x-1}, && \text{[monotonía de } \cdot \text{ (con } x \neq 1) \text{ en } \mathbb{Q}] \end{aligned}$$

de donde existe el simétrico de todos salvo del 1 (anula el denominador) y por tanto, $(\mathbb{Q}; *)$ no es grupo —$(\mathbb{Q} \setminus \{1\}; *)$ sí lo es—.

1. Cualquiera de los grupos finitos estudiados serviría de ejemplo. Fijémonos, por ejemplo en los de orden 1 y 2:

 0. El único grupo de orden 1 es C_1, el grupo cíclico,

*	e
e	e

 que en nuestro caso es

*	0
0	0

 1. El único grupo de orden 2 es C_2, el grupo cíclico,

*	0	a
0	0	a
a	a	0

del que un modelo, en nuestro caso es $(A;*)$, con $A = \{0, 2\}$; su tabla de Cayley, por definición de $*$, es

$*$	0	2
0	0	2
2	2	0

La elección de 2 proviene de exigir que cada elemento sea su propio simétrico: $x = \dfrac{x}{x-1}$, esto es, $x(x-2) = 0$, es decir, $x = 0$ o $x = 2$.

Respecto de la estructura de $(A;*)$, observemos que: como todos los elementos de la tabla son de A, $(A;*)$ es un magma; por serlo en $\mathbb{Q}$, $*$ es conmutativa, por lo que $(A;*)$ es un magma abeliano; por serlo en $\mathbb{Q}$, $*$ es asociativa en A, por lo que $(A;*)$ es un semigrupo abeliano; el elemento neutro de $*$ en $\mathbb{Q}$, 0, está en A, por lo que $(A;*)$ es un monoide abeliano, y por ser distintos de 1, todo elemento de A tiene simétrico: $0' = \dfrac{0}{0-1} = 0$ y $2' = \dfrac{2}{2-1} = 2$. ■

Ejemplo 477

Sean $2^{\{x,y\}}$ el conjunto de todos los subconjuntos de $\{x, y\}$ y Δ la diferencia simétrica de conjuntos.

0. Hallemos razonadamente la tabla de Cayley de Δ en $2^{\{x,y\}}$.
1. Demostremos que $\left(2^{\{x,y\}}; \Delta\right)$ tiene estructura de: I) magma, II) semigrupo, III) monoide, IV) grupo.
2. ¿Es $\left(2^{\{x,y\}}; \Delta\right)$ un grupo abeliano?
3. ¿A cuál es isomorfo $\left(2^{\{x,y\}}; \Delta\right)$, al grupo cíclico C_4 o al grupo de Klein K_4? ¿Por qué?

Nota.— En este ejemplo, para responder a los apartados 1, 2 y 3, podemos razonar con la tabla de Cayley hallada en el apartado 0.

[EFO 27.5.2025:4], [EFE 18.6.2025:4].

Resolución.—

0. De acuerdo a la definición de la ley de composición Δ y a la construcción

Δ	$\dots$	j	$\dots$
$\vdots$	$\dots$	$\vdots$	$\dots$
i	$\dots$	$i\Delta j$	$\dots$
$\vdots$	$\dots$	$\vdots$	$\dots$

la tabla de Cayley de Δ en $2^{\{x,y\}}$ es

Δ	$\emptyset$	$\{x\}$	$\{y\}$	$\{x,y\}$
$\emptyset$	$\emptyset$	$\{x\}$	$\{y\}$	$\{x,y\}$
$\{x\}$	$\{x\}$	$\emptyset$	$\{x,y\}$	$\{y\}$
$\{y\}$	$\{y\}$	$\{x,y\}$	$\emptyset$	$\{x\}$
$\{x,y\}$	$\{x,y\}$	$\{y\}$	$\{x\}$	$\emptyset$

ya que: $X\Delta X = (X \setminus X) \cup (X \setminus X) = \emptyset \cup \emptyset = \emptyset$ (la diferencia simétrica entre iguales es vacía); $X\Delta\emptyset = (X \cup \emptyset) \setminus (X \cap \emptyset) = X \setminus \emptyset = X$ (la diferencia simétrica con el vacío es el propio conjunto); si $Y \subseteq X$, entonces $X\Delta Y = (X \cup Y) \setminus (X \cap Y) = X \setminus Y$ (la diferencia simétrica con un subconjunto es el complementario del subconjunto en el conjunto), y si $X \cap Y = \emptyset$, entonces $X\Delta Y = (X \cup Y) \setminus (X \cap Y) = (X \cup Y) \setminus \emptyset = X \cup Y$ (la diferencia simétrica entre conjuntos disjuntos es su unión).

1. I. $(2^{\{x,y\}}; \Delta)$ *tiene estructura de magma*. En efecto, la ley de composición Δ es una operación en $2^{\{x,y\}}$ ya que, como puede verse en la tabla de Cayley, todos los resultados son elementos de $2^{\{x,y\}}$.

II. $(2^{\{x,y\}}; \Delta)$ *tiene estructura de semigrupo*. Como hemos demostrado ya que tiene estructura de magma, sólo necesitamos demostrar que Δ es asociativa en A, demostración que puede verse en el apartado 2 del ejemplo 451 (pág. 860 de esta edición).

III. $(2^{\{x,y\}}; \Delta)$ *tiene estructura de monoide*. Como hemos demostrado ya que tiene estructura de semigrupo, sólo necesitamos demostrar que existe el elemento neutro en $2^{\{x,y\}}$ para Δ. En efecto, observando la tabla de Cayley: la primera fila es copia literal de la fila de cabecera, esto es, $(\forall S \in 2^{\{x,y\}})(\emptyset\Delta S = S)$, es decir, $\emptyset$ es el neutro por la izquierda de Δ en $2^{\{x,y\}}$; análogamente, la primera columna es copia literal de la columna de cabecera, esto es, $(\forall S \in 2^{\{x,y\}})(S\Delta\emptyset = S)$, es decir, $\emptyset$ es el neutro por la derecha de Δ en $2^{\{x,y\}}$. Al ser $\emptyset$ el neutro por la izquierda y por la derecha de Δ en $2^{\{x,y\}}$, es el neutro de Δ en $2^{\{x,y\}}$.

IV. $(2^{\{x,y\}}; \Delta)$ *tiene estructura de grupo*, pues todos sus elementos son simetrizables respecto de Δ en $2^{\{x,y\}}$:

$$\begin{aligned}
&\text{de } \emptyset\Delta\emptyset = \emptyset, \text{ se sigue } \emptyset^{-1} = \emptyset;\\
&\text{de } \{x\}\Delta\{x\} = \emptyset, \text{ se sigue } \{x\}^{-1} = \{x\};\\
&\text{de } \{y\}\Delta\{y\} = \emptyset, \text{ se sigue } \{y\}^{-1} = \{y\};\\
&\text{de } \{x,y\}\Delta\{x,y\} = \emptyset, \text{ se sigue } \{x,y\}^{-1} = \{x,y\}.
\end{aligned}$$

Conclusión. De I, II, III y IV se sigue que $(2^{\{x,y\}}; \Delta)$ tiene estructura de grupo.

2. El hecho de ser la tabla de CAYLEY simétrica respecto de la diagonal principal demuestra que Δ es conmutativa en $2^{\{x,y\}}$; en otras palabras, $\left(2^{\{x,y\}};\Delta\right)$ es un grupo abeliano[21].

3. El orden de un grupo finito es su número de elementos, luego $\left(2^{\{x,y\}};\Delta\right)$ es de orden 4. Únicamente existen dos grupos no isomorfos de orden 4, el cíclico C_4 —siendo un ejemplo de modelo suyo el grupo $(\mathbb{Z}_4;+_4)$— y el de KLEIN K_4 —siendo un ejemplo de modelo suyo el grupo, con la operación composición, de las isometrías planas que dejan fijo el rectángulo no cuadrado—.

$C_4 =$

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$K_4 =$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Como $\left(2^{\{x,y\}};\Delta\right)$ es de orden 4, o bien es isomorfo a C_4 o bien es isomorfo a K_4.

Veamos ahora a cuál. Estudiémoslo de dos formas alternativas.

De una.

Observamos que todos los elementos de K_4 tienen orden 2, esto es, todos los elementos son su propio simétrico —los grupos que satisfacen esto se denominan *grupos booleanos*[22]—. Resulta que esto es lo que sucede en $\left(2^{\{x,y\}};\Delta\right)$, por lo que es isomorfo a K_4.

De otra.

Comparando las tablas, vemos que es isomorfo a K_4, el grupo no cíclico más pequeño.

$(K_4;*) =$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\left(2^{\{x,y\}};\Delta\right) =$

Δ	$\emptyset$	$\{x\}$	$\{y\}$	$\{x,y\}$
$\emptyset$	$\emptyset$	$\{x\}$	$\{y\}$	$\{x,y\}$
$\{x\}$	$\{x\}$	$\emptyset$	$\{x,y\}$	$\{y\}$
$\{y\}$	$\{y\}$	$\{x,y\}$	$\emptyset$	$\{x\}$
$\{x,y\}$	$\{x,y\}$	$\{y\}$	$\{x\}$	$\emptyset$

Como puede verse en estas tablas, la biyección $f:(K_4;*)\longrightarrow(2^{\{x,y\}};\Delta)$ definida por $f(e)=\emptyset$, $f(a)=\{x\}$, $f(b)=\{y\}$, $f(c)=\{x,y\}$, satisface $\forall\alpha,\beta\in K_4$, $f(\alpha*\beta)=f(\alpha)\Delta f(\beta)$ —a modo de ejemplo, $f(a*b)=f(c)=\{x,y\}=\{x\}\Delta\{y\}=f(a)\Delta f(b)$—, por lo que es un isomorfismo de grupos[23]. ■

[21] Quizás hubiese sido más sencillo decir que $\left(2^{\{x,y\}};\Delta\right)$ es un grupo finito de orden 4 y que sólo existen, salvo isomorfismos, dos de tales grupos, C_4 y K_4, ambos abeliianos.

[22] *Vid. v. gr.* https://en.wikipedia.org/wiki/Elementary_abelian_group.

[23] Alternativamente, observemos que todos los elementos de la diagonal principal de $(K_4;*)$ son el elemento neutro, e, al igual que sucede con $\emptyset$ en $\left(2^{\{x,y\}};\Delta\right)$; de que esto sucede en K_4, de que no sucede en C_4 y de que C_4 y K_4 son los únicos grupos finitos de orden 4, ya pudiésemos deducir la isomorfía.

Actividad 17.7

Hagamos todo lo propuesto en el ejemplo anterior para la estructura $\left(2^{\{x,y\}};\Delta^{\complement}\right)$, siendo $\Delta^{\complement}$ la operación complementario de la diferencia simétrica.

Con miras a su resolución.— La tabla de Cayley es

$$\left(2^{\{x,y\}};\Delta^{\complement}\right)=\begin{array}{c|cccc}\Delta^{\complement} & \emptyset & \{x\} & \{y\} & \{x,y\}\\ \hline \emptyset & \{x,y\} & \{y\} & \{x\} & \emptyset\\ \{x\} & \{y\} & \{x,y\} & \emptyset & \{x\}\\ \{y\} & \{x\} & \emptyset & \{x,y\} & \{y\}\\ \{x,y\} & \emptyset & \{x\} & \{y\} & \{x,y\}\end{array}$$

siendo conmutativa, el neutro $\{x,y\}$ y cada uno su inverso.

Actividad 17.8

Demostremos que ni Δ se distribuye en $\Delta^{\complement}$ ni $\Delta^{\complement}$ se distribuye en Δ.

Actividad 17.9

A la vista de las tablas, las acciones de Δ y $\Delta^{\complement}$ en $2^{\{x,y\}}$ parecen que pudiesen relacionarse con la disyunción y la equivalencia, respectivamente, pero ¿en una lógica bivalente, trivalente o tetravalente?

§ 17.6.10 Cuadrado latino. Cuasigrupo

Definición 17.46.— Un *cuadrado latino* es una malla cuadrada de celdas que contiene exactamente un símbolo en cada fila y cada columna.

Definición 17.47.— Decimos que un magma $(X;*)$ satisface la *propiedad del cuadrado latino* precisamente si para todo $x,y\in X$, existen dos únicos elementos $z,t\in X$ tales que $x*z=y$, $t*x=y$.

Definición 17.48.— Un *cuasigrupo* es un magma que satisface la propiedad del cuadrado latino.

Teorema 17.47

Las tablas de Cayley de un cuasigrupo y de un grupo, finitos, son cuadrados latinos.

Ejemplo 478

Tenemos dos redes de sistemas informáticos, la red A y la red B, compuestas en concreto cada una por tres sistemas, A_0, A_1 y A_2 y B_0, B_1 y B_2, respectivamente. Queremos programar la interconexión de las nueve parejas interredes $\langle A_i, B_j \rangle$. Disponemos de tres fechas t_0, t_1 y t_2, en las que ejecutar dichas interconexiones. El requisito de tener que interconectar todas las parejas no debe generar ninguna colisión entre las fechas.

Resolución.— El grupo cíclico C_3 nos permite resolver esta cuestión. Observemos el cuadrado latino de su tabla de CAYLEY modificada renombrando los elementos de sus filas y columnas,

	B_0	B_1	B_2
A_0	t_0	t_1	t_2
A_1	t_1	t_2	t_0
A_2	t_2	t_0	t_1

■

Teorema 17.48
No todo cuadrado latino es la tabla de CAYLEY de un grupo.

Ejemplo 479

En el supuesto del ejemplo anterior, nuestra meta es ahora la resolución conjunta interred de tres problemas P_0, P_1 y P_2, con el requisito de que cada sistema trabaje en un problema distinto con un sistema de la otra red.

Resolución.— El siguiente cuadrado latino —que no es un grupo— nos proporciona un camino,

	B_0	B_1	B_2
A_0	P_0	P_1	P_2
A_1	P_2	P_0	P_1
A_2	P_1	P_2	P_0

■

Ejemplo 480 Ortogonalidad

¿Pudiésemos programar conjuntamente las fechas de interconexión y la resolución de problemas? es decir, ¿pudiésemos interconectar todas las parejas sin generar ninguna colisión entre las fechas, a la vez que cada sistema trabaja en un problema distinto con un sistema de la otra red?

Resolución.— Sí, de acuerdo al cuadrado latino producto

	B_0	B_1	B_2
A_0	$\langle t_0, P_0\rangle$	$\langle t_1, P_1\rangle$	$\langle t_2, P_2\rangle$
A_1	$\langle t_1, P_2\rangle$	$\langle t_2, P_0\rangle$	$\langle t_0, P_1\rangle$
A_2	$\langle t_2, P_1\rangle$	$\langle t_0, P_2\rangle$	$\langle t_1, P_0\rangle$

■

Cuando dos cuadrados latinos pueden combinarse en esa forma, decimos que son (mutuamente) ortogonales.

Para saber más, *vid. v. gr.* https://en.wikipedia.org/wiki/Mutually_orthogonal_Latin_squares.

§ 17.7 Semianillo

Definición 17.49.— Sean $A \neq \emptyset$ y $\oplus$ y $\otimes$ dos operaciones diádicas en A. Decimos que $\otimes$ es:

a) *distributiva por la izquierda* respecto de $\oplus$, precisamente si $(\forall a, b, c \in A)(a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c))$;

b) *distributiva por la derecha* respecto de $\oplus$, precisamente si $(\forall a, b, c \in A)((a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c))$;

c) *distributiva*, precisamente si es distributiva por la izquierda y por la derecha.

Observación 17.7.0.— También suele decirse que «$\otimes$ se distribuye (por la izqda./por la dcha.) en $\oplus$».

Actividad 17.10

Demostremos que en $\mathbb{R}^n$, tanto el producto escalar como el producto vectorial se distribuyen en la suma.

Definición 17.50.— Sean $A \neq \emptyset$ y $\oplus$ y $\otimes$ dos operaciones diádicas en A. Decimos que $(A; \oplus, \otimes)$ tiene estructura de *semianillo*, precisamente si $(A; \oplus)$ es monoide abeliano, $(A; \otimes)$ es semigrupo y $\otimes$ es distributiva respecto a $\oplus$.

Definición 17.51.— Decimos que un semianillo $(A; \oplus, \otimes)$, es un *semianillo abeliano o conmutativo*, precisamente si $\otimes$ es conmutativa, es decir, si, y sólo si,

$$(\forall a, b, c \in A)(a \otimes b = b \otimes a).$$

Definición 17.52.— Decimos que un semianillo $(A; \oplus, \otimes)$ es un *semianillo unitario* precisamente si $(A; \otimes)$ es monoide.

Ejemplo 481 (Algunos modelos de semianillos conmutativos y unitarios)

0. Dado un conjunto C, $(\mathcal{P}(C); \cup, \cap)$ es un semianillo conmutativo y unitario.
1. Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, se satisface que $(\mathbb{N}; +, \cdot)$, $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$, $(\mathbb{R}; +, \cdot)$ y $(\mathbb{C}; +, \cdot)$ son semianillos conmutativos y unitarios.

Actividad 17.11

Demostremos que en un semianillo $(A; \oplus, \otimes)$ el elemento neutro de $\oplus$ es un elemento absorbente para $\otimes$.

§ 17.8 Anillo

Definición 17.53.— Decimos que un semianillo $(A; \oplus, \otimes)$ es un *anillo*, precisamente si $(A; \oplus)$ es grupo abeliano.

Dicho de otro modo, si A es un conjunto no vacío y $\oplus$ y $\otimes$ dos operaciones diádicas en A, decimos que la terna $(A; \oplus, \otimes)$ es un *anillo* si, y sólo si, se satisface:

0.°, $(A; \oplus)$ es grupo abeliano;

1.°, $(A; \otimes)$ es un semigrupo;

2.°, $\otimes$ se distribuye en $\oplus$, esto es, $\forall x, y, z \in A$:

$$x \otimes (y \oplus z) = (x \otimes y) \oplus (x \otimes z)$$
$$\wedge$$
$$(x \oplus y) \otimes z = (x \otimes z) \oplus (y \otimes z).$$

Definición 17.54.— Decimos que un anillo $(A; \oplus, \otimes)$, es un *anillo abeliano* (o, sinónimamente, *anillo conmutativo*), precisamente si $\otimes$ es conmutativa, es decir, si, y sólo si,

$$(\forall a, b, c \in A)(a \otimes b = b \otimes a).$$

Definición 17.55.— En un anillo $(A; \oplus, \otimes)$, puede definirse una nueva operación diádica, la *sustracción* (o, sinónimamente, *diferencia*), que notamos $\ominus$, como

$$a \ominus b = a \oplus (-b),$$

donde $-b$ es el elemento opuesto de b.

Definición 17.56.— Sean $(A;\oplus,\otimes)$ un anillo y $a\in A$. Decimos que a es *nilpotente* precisamente si

$$(\exists n\in\mathbb{Z}^+)(a\otimes\overset{n}{\smile}\cdots\otimes a=e_\oplus).$$

Observación 17.8.0.— Con la notación $(A;+,\cdot)$, x es nilpotente si, y sólo si, $\exists n\in\mathbb{Z}^+$, $a\cdot\overset{n}{\cdots}\cdot a=0$, esto es, usando la notación habitual de potencias, si, y sólo si, $\exists n\in\mathbb{Z}^+$, $a^n=0$.

Definición 17.57.— Sea $(A;\oplus,\otimes)$ un anillo; el elemento a de A es *idempotente* si, y sólo si, $a\otimes a=a$.

Ejemplo 482 (Idempotencia en los anillos de los enteros, racionales y reales)

Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, se satisface:

- en los anillos abelianos $(\mathbb{Z};+,\cdot)$, $(\mathbb{Q};+,\cdot)$ y $(\mathbb{R};+,\cdot)$, sólo 0 y 1 son idempotentes.

§ 17.8.0 Anillo unitario

Definición 17.58.— Decimos que un anillo $(A;\oplus,\otimes)$ es un *anillo unitario*, precisamente si $(A;\otimes)$ es un monoide.

Teorema 17.49

Sea $(A;\oplus,\otimes)$ un anillo; se satisface:

0. $\forall a\in A$, $e_\oplus\otimes a=a\otimes e_\oplus=e_\oplus$ (esto es, el elemento neutro de $\oplus$ en A es un elemento singular o absorbente para $\otimes$ en A);
1. $\forall a,b\in A$, $(-a)\otimes b=a\otimes(-b)=-(a\otimes b)$;
2. $\forall a,b,c\in A$, $a\otimes(b\ominus c)=(a\otimes b)\ominus(a\otimes c)$.

Observación 17.8.1.— 0. En un anillo, el *elemento neutro aditivo* $e_\oplus$ suele notarse por 0 y si se trata de un anillo unitario, el *elemento neutro multiplicativo* $e_\otimes$ suele notarse por 1.

1. De hecho, la notación habitual para un anillo es $(A;+,\cdot)$, esto es, simplemente $+$ para la ley aditiva $\oplus$ y $\cdot$ para la multiplicativa $\otimes$ —y simplemente $-$ para la diferencia $\ominus$—. Así, por ejemplo, (17.49.a) quedaría: $\forall a\in A$, $0\cdot a=a\cdot 0=0$. Muchas veces incluso se suprime $\cdot$; por ejemplo, (17.49.c) quedaría: $\forall a,b,c\in A$, $a(b-c)=ab-ac$.

Unidades de un anillo unitario

Definición 17.59.— Si $(A;\oplus,\otimes)$ es un anillo unitario, entonces puede que existan elementos que tengan simétricos multiplicativos, esto es, elementos $a\in A$ para los que exista un $b\in A$ tal que

$a \otimes b = b \otimes a = 1$. Llamamos *unidades* del anillo a estos elementos del anillo que tienen simétrico multiplicativo.

Ejemplo 483 (Unidades de los anillos de los enteros, racionales, reales y complejos)

Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, se satisface:

- $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$, $(\mathbb{R}; +, \cdot)$ y $(\mathbb{C}; +, \cdot)$ son anillos conmutativos y unitarios;
- en $(\mathbb{Z}; +, \cdot)$ sólo hay una unidad, el 1;
- en $(\mathbb{Q}; +, \cdot)$, $(\mathbb{R}; +, \cdot)$ y $(\mathbb{C}; +, \cdot)$, todos los elementos no nulos son unidades del anillo.

Característica de un anillo unitario

Definición 17.60.— Sea $(A; \oplus, \otimes)$ un anillo unitario; decimos que es un *anillo de característica* $p \in \mathbb{Z}^+$ si p es el menor natural tal que $e_\otimes \oplus \overset{p}{\overbrace{\cdots}} \oplus e_\otimes = e_\oplus$. Si no existe tal p decimos que el anillo tiene característica 0.

Ejemplo 484

Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, demostremos que $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$ y $(\mathbb{R}; +, \cdot)$ son anillos de característica 0.

Resolución.— Ciertamente, pues para ninguno de ellos es posible encontrar un $p \in \mathbb{Z}^+$ tal que $1 + \overset{p}{\overbrace{\cdots}} + 1 = 0$, ya que de $p \cdot 1 = 0$, necesariamente $p = 0$. · ■

§ 17.8.1 Subanillo

Definición 17.61.— Sean $(A; \oplus, \otimes)$ un anillo y $S \subseteq A$. Decimos que $(S; \oplus, \otimes)$ es un *subanillo* del anillo $(A; \oplus, \otimes)$ precisamente si $(S; \oplus, \otimes)$ es anillo.

Teorema 17.50 (Caracterización de subanillo)
Sean $(A; \oplus, \otimes)$ un anillo y $S \subseteq A$, $S \neq \emptyset$. $(S; \oplus, \otimes)$ es subanillo de $(A; \oplus, \otimes)$ si, y sólo si,

$$(\forall x, y \in S)(x \oplus (-y) \in S)$$
$$\wedge$$
$$(\forall x, y \in S)(x \otimes y \in S).$$

Ejemplo 485 (Algunos modelos de subanillos)

Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, se satisface:

- $(\mathbb{Z}; +, \cdot)$ es subanillo de $(\mathbb{Q}; +, \cdot)$;
- $(\mathbb{Z}; +, \cdot)$ es subanillo de $(\mathbb{R}; +, \cdot)$;
- $(\mathbb{Q}; +, \cdot)$ es subanillo de $(\mathbb{R}; +, \cdot)$.

§ 17.8.2 Ideal

Definición 17.62.— Sea $(A; \oplus, \otimes)$ un anillo. Decimos que un subgrupo $(I; \oplus)$ de $(A; \oplus)$ es un:

a) *ideal por la izquierda* de $(A; \oplus)$ si, y sólo si, $\forall x \in I, \forall a \in A, a \otimes x \in I$;

b) *ideal por la derecha* de $(A; \oplus)$ si, y sólo si, $\forall x \in I, \forall a \in A, x \otimes a \in I$;

c) *ideal* si, y sólo si, es un ideal por la izquierda y por la derecha.

Definición 17.63.— Decimos que el ideal I es un *ideal propio* precisamente si $I \neq \{0\}$ e $I \neq A$.

Definición 17.64.— Todo elemento x de A genera un ideal de A, que designamos por xA, que es $xA = \{xa : a \in A\}$. De un ideal generado de esta forma decimos que es un *ideal principal*.

Definición 17.65.— Decimos que A es un *anillo principal* precisamente si todos sus ideales son principales.

Ejemplo 486

Demostremos que $\mathbb{Z}$ con las operaciones habituales es un anillo principal.

Resolución.— Lo es, porque los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, ya que los únicos subgrupos aditivos de $\mathbb{Z}$ son los generados por un elemento. Claramente $n\mathbb{Z}$ es un ideal de $\mathbb{Z}$, pues si $m \in \mathbb{Z}$ y $nk \in n\mathbb{Z}$, entonces $m(nk) = (mn)k = (nm)k = n(mk) \in n\mathbb{Z}$ ($n\mathbb{Z}$ es ideal por la izquierda) y $(nk)m = n(km) \in n\mathbb{Z}$ ($n\mathbb{Z}$ es ideal por la derecha). Y son los únicos subgrupos, pues, por un lado, si un subgrupo S es $\{0\}$, entonces es $S = 0\mathbb{Z}$, y, por otro, veamos qué pasa si $S \neq \{0\}$. En este caso, esperaremos a estudiar el algoritmo de la división euclidea[24], tras lo que pudiésemos retomar esta demostración como una actividad, con la sugerencia de, seleccionando un entero positivo n, aplicar reducción al absurdo suponiendo que existen elementos en el subgrupo que no son divisibles por n. No es difícil, lo dicho, pudiésemos demostrarlo como actividad práctica (✍). ∎

[24] *Vid. infra* definición 18.8 (pág. 949 de esta edición).

§ 17.8.3 Homomorfismo de anillos

Definición 17.66.— Sean $(A_0; \oplus, \otimes)$ y $(A_1; \boxplus, \boxtimes)$ dos anillos y $f : A_0 \longrightarrow A_1$ una aplicación. Decimos que f es un *homomorfismo de anillos* precisamente si $\forall a, b \in A_0$ se satisfacen:

$$f(a \oplus b) = f(a) \boxplus f(b),$$
$$f(a \otimes b) = f(a) \boxtimes f(b).$$

Teorema 17.51
Sean $(A_0; \oplus, \otimes)$ y $(A_1; \boxplus, \boxtimes)$ dos anillos y $f : A_0 \longrightarrow A_1$ un homomorfismo de anillos. Se satisface que toda imagen (resp., contraimagen) de un subanillo de A_0 (resp., A_1) es un subanillo de A_1 (resp., A_0).

Definición 17.67.— Sean $(A_0; \oplus, \otimes)$ y $(A_1; \boxplus, \boxtimes)$ dos anillos y $f : A_0 \longrightarrow A_1$ un homomorfismo de anillos.

0. Llamamos *núcleo de* f y lo designamos por $\ker f$, al subconjunto de A_0:

$$\ker f = \{x \in A_0 : f(x) = e_{\boxplus}\} .$$

1. Llamamos *imagen* de f y lo designamos por $\operatorname{im} f$ (o por $f(A_0)$) al subconjunto de A_1:

$$\operatorname{im} f = \{y \in A_1 : \exists x \in A_0, f(x) = y\} .$$

Teorema 17.52
Sean $(A_0; \oplus, \otimes)$ y $(A_1; \boxplus, \boxtimes)$ dos anillos y $f : A_0 \longrightarrow A_1$ un homomorfismo de anillos. Se satisface:

0. $\ker f$ es un ideal de $(A_0; \oplus, \otimes)$;
1. $\operatorname{im} f$ es un subanillo de $(A_1; \boxplus, \boxtimes)$.

Teorema 17.53
Sean $(A_0; \oplus, \otimes)$ y $(A_1; \boxplus, \boxtimes)$ dos anillos. Se satisface:

0. $f : A_0 \longrightarrow A_1$ es *monomorfismo* si, y sólo si, $\ker f = \{e_{\oplus}\}$;
1. $f : A_0 \longrightarrow A_1$ es *epimorfismo* si, y sólo si, $\operatorname{im} f = A_1$.

Definición 17.68 (Anillo cociente módulo un ideal).— Sean $(A; \oplus, \otimes)$ un anillo e $(I; \oplus, \otimes)$ un ideal suyo. Sea $C = \{a + I : a \in A\}$ el conjunto de las clases de A módulo I. Llamamos *anillo cociente* de A módulo I y lo designamos por A/I, al anillo $(A; +, \cdot)$, donde:

- la operación aditiva, $+$, se define, $\forall a+I, b+I \in A$, por $(a+I)+(b+I)=(a+b)+I$, y
- la operación multiplicativa, $\cdot$, se define, $\forall a+I, b+I \in A$, por $(a+I)\cdot(b+I)=(a\cdot b)+I$.

Teorema 17.54 (Descomposición canónica de un homomorfismo de anillos)
Sean $(A_0; \oplus, \otimes)$ y $(A_1; \boxplus, \boxtimes)$ dos anillos y $f : A_0 \longrightarrow A_1$ un homomorfismo de anillos. Entonces, la descomposición canónica de f es $f = n \circ g \circ i$, esto es,

$$\begin{array}{ccc} A_0 & \xrightarrow{f} & A_1 \\ \downarrow n & & \uparrow i \\ A_0/\ker f & \xrightarrow{g} & f(A_0) \end{array}$$

donde;
n es el epimorfismo definido por $n(x) = x + \ker f$;
g es el isomorfismo definido por $g(x+\ker f) = f(x)$, e
i es el monomorfismo definido por $i(x) = x$.

§ 17.8.4 Muestra de más ejemplos

Ejemplo 487 (Anillo y espacio vectorial de las funciones reales de variable real [RVR])

Sea D un subconjunto no vacío de $\mathbb{R}$. Sea $\mathcal{F}(D,\mathbb{R})$ el conjunto de todas las funciones reales de variable real con dominio D. Sean las operaciones $(f+g)(x) = f(x)+g(x)$, $(f\cdot g)(x) = f(x)\cdot g(x)$ y $(af)(x) = a\cdot f(x)$, para cualesquiera $f, g \in \mathcal{F}(D,\mathbb{R})$ y $a \in \mathbb{R}$. Entonces:

0. $\langle \mathcal{F}(D,\mathbb{R}), +\rangle$ es un grupo abeliano, el *grupo de las funciones reales de variable real definidas en* D (el elemento neutro es la función constante cero, $z(x) = 0$);
1. $\langle \mathcal{F}(D,\mathbb{R}), \cdot\rangle$ es un monoide abeliano, el *monoide de las funciones reales de variable real definidas en* D (el elemento neutro es la función constante uno, $u(x) = 1$);
2. $(\mathcal{F}(D,\mathbb{R}); +, \cdot)$ es un anillo conmutativo y unitario, el *anillo de las funciones reales de variable real definidas en* D;
3. $(\mathcal{F}(D,\mathbb{R}); +, \cdot, \mathbb{R})$ es un espacio vectorial real, el *espacio vectorial de las funciones reales de variable real definidas en* D.

Ejemplo 488 (Anillo y espacio vectorial de las funciones RVR continuas en un abierto)

Sea el intervalo abierto de números reales (a,b). Sea $\mathcal{C}((a,b),\mathbb{R})$ el conjunto de todas las funciones reales de variable real continuas en (a,b). Entonces:

0. $\langle \mathcal{C}((a,b),\mathbb{R}), +\rangle$ es un grupo abeliano, el *grupo de las funciones reales de variable real continuas en* (a,b);

1. $\langle \mathcal{C}((a,b),\mathbb{R}),\cdot\rangle$ es un monoide abeliano, el *monoide de las funciones reales de variable real continuas en* (a,b);

2. $\langle \mathcal{C}((a,b),\mathbb{R});+,\cdot\rangle$ es un anillo conmutativo y unitario, el *anillo de las funciones reales de variable real continuas en* (a,b);

3. $\langle \mathcal{C}((a,b),\mathbb{R});+,\cdot,\mathbb{R}\rangle$ es un espacio vectorial real, el *espacio vectorial de las funciones reales de variable real continuas en* (a,b).

Ejemplo 489 (Anillo y espacio vectorial de las funciones RVR derivables en un abierto)

Sea el intervalo abierto de números reales (a,b). Sea $\mathcal{D}((a,b),\mathbb{R})$ el conjunto de todas las funciones reales de variable real derivables en (a,b). Entonces:

0. $\langle \mathcal{D}((a,b),\mathbb{R}),+\rangle$ es un grupo abeliano, el *grupo de las funciones reales de variable real derivables en* (a,b);

1. $\langle \mathcal{D}((a,b),\mathbb{R}),\cdot\rangle$ es un monoide abeliano, el *monoide de las funciones reales de variable real derivables en* (a,b);

2. $\langle \mathcal{D}((a,b),\mathbb{R});+,\cdot\rangle$ es un anillo conmutativo y unitario, el *anillo de las funciones reales de variable real derivables en* (a,b);

3. $\langle \mathcal{D}((a,b),\mathbb{R});+,\cdot,\mathbb{R}\rangle$ es un espacio vectorial real, el *espacio vectorial de las funciones reales de variable real derivables en* (a,b).

Ejemplo 490 (El anillo de los polinomios con coeficientes reales)

$(\mathbb{R}[x];+,\cdot)$ con $(a_0,a_1,\ldots,a_p,0,0,\ldots)+(b_0,b_1,\ldots,b_q,0,0,\ldots)=(a_0+b_0,a_1+b_1,\ldots,a_r+b_r,0,0,\ldots)$, donde $r\leq \text{máx}(p,q)$, $(a_0,a_1,\ldots,a_p,0,0,\ldots)\cdot(b_0,b_1,\ldots,b_q,0,0,\ldots)=(a_0+a_1x+a_2x^2+\ldots+a_px^p)\cdot b_0+(a_0+a_1x+a_2x^2+\ldots+a_px^p)\cdot b_1x+(a_0+a_1x+a_2x^2+\ldots+a_px^p)\cdot b_2x^2+\ldots+(a_0+a_1x+a_2x^2+\ldots+a_px^p)\cdot b_qx^q$, $0=(0,0,\ldots)$ (polinomio cero, neutro de la suma) y $1=(1,0,0,\ldots)$ (polinomio uno, neutro del producto), es un anillo conmutativo y unitario, el *anillo de los polinomios con coeficientes reales*.

Ejemplo 491 (Anillos y espacios vectoriales de sucesiones reales)

Sean $\mathcal{S}(X)$, $\mathcal{S}_A(X)$, $\mathcal{S}_C(X)$, $\mathcal{S}_L(X)$ y $\mathcal{S}_0(X)$ los conjuntos de sucesiones, sucesiones acotadas, de Cauchy, convergentes y nulas en X. Recordemos que $\mathcal{S}_0(\mathbb{R})\subset\mathcal{S}_L(\mathbb{R})=\mathcal{S}_C(\mathbb{R})\subset\mathcal{S}_A(\mathbb{R})\subset\mathcal{S}(\mathbb{R})$ y que $\mathcal{S}_0(\mathbb{Q})\subset\mathcal{S}_L(\mathbb{Q})\subset\mathcal{S}_C(\mathbb{Q})\subset\mathcal{S}_A(\mathbb{Q})\subset\mathcal{S}(\mathbb{Q})$. Se satisface que:

0. $\langle\mathcal{S}(\mathbb{R}),+,\cdot\rangle$, $\langle\mathcal{S}_A(\mathbb{R}),+,\cdot\rangle$, $\langle\mathcal{S}_L(\mathbb{R}),+,\cdot\rangle$, $\langle\mathcal{S}_0(\mathbb{R}),+,\cdot\rangle$ son anillos conmutativos;

1. $\langle \mathcal{S}_0(\mathbb{R}), +, \cdot \rangle$ es un ideal de $\langle \mathcal{S}_A(\mathbb{R}), +, \cdot \rangle$;
2. $\langle \mathcal{S}(\mathbb{R}), +, \cdot, \mathbb{R} \rangle$, $\langle \mathcal{S}_A(\mathbb{R}), +, \cdot, \mathbb{R} \rangle$, $\langle \mathcal{S}_L(\mathbb{R}), +, \cdot, \mathbb{R} \rangle$ y $\langle \mathcal{S}_0(\mathbb{R}), +, \cdot, \mathbb{R} \rangle$ son espacios vectoriales.

§ 17.9 Anillo íntegro

Definición 17.69.— Sean $(A; \oplus, \otimes)$ un semianillo y $x \in A$. Decimos que:

0. x es *divisor de cero por la izquierda* si, y sólo si, $\exists y \neq 0, x \otimes y = 0$;
1. x es *divisor de cero por la derecha* si, y sólo si, $\exists y \neq 0, y \otimes x = 0$;
2. x es *divisor de cero* si, y sólo si, es divisor de cero por la izquierda y por la derecha.

Definición 17.70.— Decimos que un semianillo $(A; \oplus, \otimes)$ es un *semianillo íntegro*) (o, sinónimamente, *semianillo de integridad*), precisamente si no tiene divisores de cero, esto es, si, y sólo si,

$$(\forall x, y \in A)(x \otimes y = 0 \to x = 0 \vee y = 0)).$$

Ejemplo 492 (Un modelo de semianillo conmutativo, unitario e íntegro)

Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{N}$,

- $(\mathbb{N}; +, \cdot)$ es un semianillo conmutativo, unitario e íntegro.

Definición 17.71.— Decimos que un anillo $(A; \oplus, \otimes)$ es un *anillo íntegro*) (o, sinónimamente, *anillo de integridad*), precisamente si como semianillo es un semianillo íntegro.

Ejemplo 493 (Algunos modelos de anillos conmutativos, unitarios e íntegros)

Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$:

- $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$ y $(\mathbb{R}; +, \cdot)$ son anillos conmutativos, unitarios e íntegros.

§ 17.10 Dominio de integridad

Definición 17.72.— Decimos que un anillo de integridad $(A; \oplus, \otimes)$ es un *dominio de integridad*, precisamente si $(A; \otimes)$ es monoide abeliano, esto es, si, y sólo si, es un anillo conmutativo, unitario y sin divisores de cero.

Ejemplo 494 (Algunos modelos de dominios de integridad)

Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$,

- $(\mathbb{Z};+,\cdot)$, $(\mathbb{Q};+,\cdot)$ y $(\mathbb{R};+,\cdot)$ son dominios de integridad —esto es, lo que habíamos dicho en el ejemplo 493 (pág. 907 de esta edición), que son anillos conmutativos, unitarios e íntegros—.

Observación 17.10.0.— En algunos textos, se entiende por dominio de integridad un anillo conmutativo e íntegro, esto es, no se exige ser unitario.

§ 17.11 Cuerpo

Definición 17.73.— Decimos que un anillo unitario $(A;\oplus,\otimes)$ es un *cuerpo* precisamente si $(A\setminus\{0\};\otimes)$ es grupo.

Dicho de otro modo, si A es un conjunto no vacío y $\oplus$ y $\otimes$ dos operaciones en A, decimos que la terna $(A;\oplus,\otimes)$ es un *cuerpo* si, y sólo si, se satisface:

0.°, $(A;\oplus)$ es un grupo abeliano con elemento neutro 0;

1.°, $(A\setminus\{0\};\otimes)$ es un grupo;

2.°, $\otimes$ se distribuye en $\oplus$: $\forall x,y,z\in A, x\otimes(y\oplus z)=(x\otimes y)\oplus(x\otimes z)$.

Decir que un cuerpo es *abeliano* (o *conmutativo*) equivale a decir que $\otimes$ satisface la conmutativa. *Campo* suele ser sinónimo de cuerpo abeliano.

Ejemplo 495 (Algunos modelos de cuerpos conmutativos)

Siendo $+$ y $\cdot$ la suma y producto habituales en $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$,

- $(\mathbb{Q};+,\cdot)$, $(\mathbb{R};+,\cdot)$ y $(\mathbb{C};+,\cdot)$ son cuerpos conmutativos.

Observación 17.11.0.— En algunos textos, un cuerpo no conmutativo se denomina *cuerpo oblicuo* (o, sinónimamente, *hemicuerpo*).

Teorema 17.55
Todo dominio de integridad finito es un cuerpo.

Teorema 17.56
I es un ideal maximal del anillo A si, y sólo si, A/I —el anillo cociente de A módulo I— es un cuerpo.

Debemos observar que, en realidad, pudiésemos demostrar que $(\mathbb{Q}; +, \cdot)$ es el menor cuerpo que extiende al anillo $(\mathbb{Z}; +, \cdot)$, estando determinado únicamente salvo isomorfismo. De manera similar, puede completarse cualquier anillo de integridad generando su cuerpo de cocientes[25]. Una relación totalmente análoga existe entre el anillo de los polinomios $(\mathbb{R}[x]; +, \cdot)$ y el cuerpo de las razones algebraicas (cuerpo que se construye de manera similar a como se construye $\mathbb{Q}$ a partir de $\mathbb{Z}$).

Ejemplo 496 (El cuerpo de las razones algebraicas)

Sabemos que en $(\mathbb{R}[x]; +, \cdot)$ la solución de la ecuación $ff' = 1$ definitoria del inverso f' de un polinomio f obliga a que $\delta f + \delta f' = 0$ (δ designa el grado) por lo que sólo existen los inversos de los polinomios de grado cero. Se construye un cuerpo que contiene a $\mathbb{R}[x]$ y en el que todo polinomio tiene inverso. Para la construcción se define la relación de equivalencia entre fracciones algebraicas, $\frac{f}{g} \sim \frac{f'}{g'}$ si, y sólo si, $fg' = gf'$, donde $f \in \mathbb{R}[x]$ y $g \in \mathbb{R}[x] \setminus \{0\}$ y la clase de equivalencia de $\frac{f}{g}$ se designa por $\left[\frac{f}{g}\right]$ y el conjunto cociente por $\mathbb{R}(x)$. Así, $(\mathbb{R}(x); +, \cdot)$ con $\left[\frac{f}{g}\right] + \left[\frac{f'}{g'}\right] = \left[\frac{fg' + f'g}{gg'}\right]$, $\left[\frac{f}{g}\right] \cdot \left[\frac{f'}{g'}\right] = \left[\frac{ff'}{gg'}\right]$, $\left[\frac{0}{g}\right]$ (razón cero, neutro de la suma) y $\left[\frac{1}{1}\right]$ (razón uno, neutro del producto), es un cuerpo conmutativo, el *cuerpo de las razones algebraicas*.

Teorema 17.57
Se satisface:

0. Todo cuerpo es un dominio de integridad.
1. Todo dominio de integridad es un anillo conmutativo.
2. Todo dominio de integridad es un anillo unitario.

Teorema 17.58
Todo anillo unitario contenido en un cuerpo es un dominio de integridad.

§ 17.11.0 Subcuerpo

Definición 17.74.— Sean $(K; \oplus, \otimes)$ un cuerpo y $S \subseteq K$. Decimos que $(S; \oplus, \otimes)$ es un *subcuerpo* del cuerpo $(K; \oplus, \otimes)$ precisamente si $(S; \oplus, \otimes)$ es cuerpo.

[25] *Vid. infra* § 17.11.2 (pág. 910 de esta edición).

Teorema 17.59 (Caracterización de subcuerpo)
Sean $(K;\oplus,\otimes)$ un cuerpo y $S\subseteq K, S\neq\emptyset$. Entonces $(S;\oplus,\otimes)$ es subcuerpo de $(K;\oplus,\otimes)$ precisamente si

$$(\forall x,y\in S)(x\oplus(-y)\in S)$$
$$\wedge$$
$$(\forall x,y\in S\setminus\{0\})(x\otimes y^{-1}\in S\setminus\{0\}).$$

§ 17.11.1 Característica de un cuerpo

Definición 17.75.— Decimos que $(\mathbb{K};\oplus,\otimes)$ es un *cuerpo de característica* $p\in\mathbb{N}$ si p es el menor natural tal que $1\oplus\overset{p}{\cdots}\oplus 1=0$. Si no existe tal p, decimos que el cuerpo tiene característica 0.

Ejemplo 497 (Algunos modelos de cuerpos de característica 0)

Siendo $+$ y $\cdot$ la suma y producto habituales en estos conjuntos:

- $(\mathbb{Q};+,\cdot)$ y $(\mathbb{R};+,\cdot)$ son cuerpos de característica 0.

§ 17.11.2 Cuerpo de cocientes de un dominio de integridad

Cualquier dominio de integridad puede ser encajado en un cuerpo, vía la estructura del cuerpo de cocientes, que precisamente resulta ser el cuerpo más pequeño que lo embebe.

Sea $(A;\oplus,\otimes)$ un dominio de integridad. Consideremos en $A\times A^*$ la relación

$$(\forall\langle a,b\rangle,\langle c,d\rangle\in A\times A^*)(\langle a,b\rangle E\langle c,d\rangle\leftrightarrow a\cdot d=b\cdot c),$$

que es de equivalencia.

Suele designarse por $Q(A)$ el conjunto cociente, esto es,

$$Q(A)={}^{A\times A^*}\!/_{E},$$

y por $\dfrac{a}{b}$, la clase de equivalencia $[\langle a,b\rangle]$.

Las operaciones diádicas en $Q(A)$ se definen en función de las del dominio de integridad $(A;\oplus,\otimes)$, así, $\forall[\langle a,b\rangle],[\langle c,d\rangle]\in Q(A)$,

$$[\langle a,b\rangle]\boxplus[\langle c,d\rangle]=[(a\otimes d\oplus b\otimes c,b\otimes d)]$$
$$[\langle a,b\rangle]\boxtimes[\langle c,d\rangle]=[(a\otimes c,b\otimes d)]$$

Pudiésemos demostrar que $(Q(A);\boxplus,\boxtimes)$ tiene estructura de cuerpo.

§ 17.11.3 Homomorfismo de cuerpos

Definición 17.76.— Sean $(K_0; \oplus, \otimes)$ y $(K_1; \boxplus, \boxtimes)$ dos cuerpos y $f : K_0 \longrightarrow K_1$ una aplicación. Decimos que f es un *homomorfismo de cuerpos* precisamente si lo es como homomorfismo de anillos.

§ 17.12 Estructuras ordenadas

§ 17.12.0 Isotonía

Definición 17.77.— Sea $(A; *)$ un magma y R una relación diádica en A. Decimos que:

0. R es *isótona* (o, sinónimamente, *compatible* o *monótona*) *por la izquierda* con $*$ si, y sólo si,

$$(\forall a, b, c \in A) \, (aRb \rightarrow (c * a) \, R \, (c * b)) \, ;$$

1. R es *isótona* (o, sinónimamente, *compatible* o *monótona*) *por la derecha* con $*$ si, y sólo si,

$$(\forall a, b, c \in A) \, (aRb \rightarrow (a * c) \, R \, (b * c)) \, ;$$

2. R es *isótona* (o, sinónimamente, *compatible* o *monótona*) con $*$ (o simplemente que R y $*$ *son compatibles*) si, y sólo si,

$$(\forall a, b, c, d \in A) \, (aRb \wedge cRd \rightarrow (a * c) \, R \, (b * d)) \, .$$

Teorema 17.60

Sea $(A; *)$ un magma y R una relación diádica en A. Entonces se satisface que:

0. si R es isótona y reflexiva, entonces es isótona por la izquierda y por la derecha;
1. si R es isótona por la izquierda y por la derecha y es transitiva, entonces es isótona.

Observación 17.12.0.— Notemos que si una relación diádica R es reflexiva y transitiva (en particular, si R es de equivalencia o de orden), entonces ser R isótona equivale a ser R isótona a la vez por la izquierda y por la derecha.

Ejemplo 498

La relación en $\mathbb{Z}$ definida $\forall x, y \in \mathbb{Z}$ por

$$xRy \leftrightharpoons x - y \text{ es múltiplo de } n,$$

es una relación de equivalencia en $\mathbb{Z}$. Demostremos que esta relación es isótona tanto con la suma como con el producto de números enteros.

Resolución.— En efecto, dados $a, b, c, d \in \mathbb{Z}$, $aRb \leftrightarrow (\exists h \in \mathbb{Z})(a - b = hn)$, y $cRd \leftrightarrow (\exists k \in \mathbb{Z})(c - d = kn)$, esto es, $a = hn + b$ y $c = kn + d$, de donde: 0.º, $(a + c) - (b + d) = b + hn + kn + d - b - d = (h + k)n$, por lo que R es isótona con la suma, y 1.º, $ac - bd = (b + hn)(kn + d) - bd = bkn + bd + hnkn + hnd - bd$, por lo que R es isótona con el producto. ∎

Teorema 17.61
Sea $(A; *)$ un magma y R una relación diádica de equivalencia en A, isótona con $*$. La ley de composición diádica $\bar{*}$ definida en el conjunto cociente A/R por, $\forall [a], [b] \in A/R$

$$[a]\bar{*}[b] = [a * b],$$

es una operación en A/R.

Definición 17.78.— La ley $\bar{*}$ se conoce como la *ley cociente* de $*$ según R.

Teorema 17.62
Sea $(A; *)$ un magma y R una relación diádica de equivalencia en A, isótona con $*$. Se satisface:

0. si $*$ es conmutativa en A, entonces $\bar{*}$ es conmutativa en A/R;
1. si $*$ es asociativa en A, entonces $\bar{*}$ es asociativa en A/R;
2. si e es el elemento neutro de $*$ en A, entonces $[e]$ es el elemento neutro de $\bar{*}$ en A/R;
3. si $a\prime$ es el simétrico de a respecto de $*$ en A, entonces $[a\prime]$ es el simétrico de $[a]$ respecto de $\bar{*}$ en A/R.

Ejemplo 499 ($\mathbb{Z}/n\mathbb{Z}$)

El conjunto cociente de la relación en $\mathbb{Z}$ definida $\forall x, y \in \mathbb{Z}$ por $xRy \leftrightharpoons x - y$ es múltiplo de n, es

$$\mathbb{Z}/R = \{[0]_{(n)}, [1]_{(n)}, [2]_{(n)}, \ldots, [n-1]_{(n)}\}.$$

Este conjunto cociente se designa por $\mathbb{Z}/n\mathbb{Z}$ —o, sinónimamente, por $\mathbb{Z}/(n)$, o incluso, con frecuencia, simplemente por $\mathbb{Z}_n$ (aunque éste puede confundirse con el conjunto de números n-ádicos)—; las clases también se designan sin los subíndices si no hay lugar a error.

Como la relación R es isótona con la suma y también con el producto de números enteros, es posible definir las leyes cocientes de las operaciones suma y producto de números enteros, $+$ y $\cdot$, según la relación R anterior —las operaciones suma $+_n$ y producto $\cdot_n$ en $\mathbb{Z}/n\mathbb{Z}$— por, $\forall [x], [y] \in \mathbb{Z}/n\mathbb{Z}$,

$$[x] +_n [y] = [x + y] = \{z \in \mathbb{Z} : x + y - z \text{ es múltiplo de } n\},$$
$$[x] \cdot_n [y] = [x \cdot y] = \{z \in \mathbb{Z} : x \cdot y - z \text{ es múltiplo de } n\}.$$

A modo de ejemplo, para el caso concreto de $n = 7$, $[3] +_7 [4] = [3 + 4] = [7] = \{z \in \mathbb{Z} : 7 - z \text{ es múltiplo de } 7\} = \{\ldots, -21, -14, -7, 0, 7, 14, 21, \ldots\} = [0]$ y $[3] \cdot_7 [5] = [3 \cdot 5] = [15] = \{z \in \mathbb{Z} : 15 - z \text{ es múltiplo de } 7\} = \{\ldots, -20, -13, -6, 1, 8, 15, 22, \ldots\} = [1]$. Las tablas de composición de $(\mathbb{Z}_7; +_7)$ y $(\mathbb{Z}_7; \cdot_7)$ son las siguientes, en las que destacamos que $[3] +_7 [4] = [0]$ y $[3] \cdot_7 [5] = [1]$ (es habitual relajar la notación y que aparezcan los números sin sus marcas de clases de equivalencia).

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Observación 17.12.1.— De hecho, $(\mathbb{Z}/n\mathbb{Z}; +_n, \cdot_n)$ tiene estructura de anillo abeliano, esto es, $(\mathbb{Z}/n\mathbb{Z}; +_n)$ es grupo abeliano, $(\mathbb{Z}/n\mathbb{Z}; \cdot_n)$ es semigrupo abeliano y $+_n$ se distribuye en $\cdot_n$.

En realidad, $(\mathbb{Z}/n\mathbb{Z}; +_n, \cdot_n)$ es el anillo cociente de $\mathbb{Z}$ por el ideal $n\mathbb{Z}$, y $(\mathbb{Z}/n\mathbb{Z}; +_n)$ es el grupo cociente de $\mathbb{Z}$ por el subgrupo normal $n\mathbb{Z}$.

En general, $(\mathbb{Z}/n\mathbb{Z}; +_n, \cdot_n)$ no es un anillo íntegro. A modo de ejemplo, 2 y 3 son divisores de cero en $(\mathbb{Z}/6\mathbb{Z}; +_6, \cdot_6)$, ya que $2 \cdot_6 3 = 0$.

$(\mathbb{Z}/n\mathbb{Z}; +_n, \cdot_n)$ es un anillo íntegro si, y sólo si, n es un número primo.

Un número $m \in \mathbb{Z}/n\mathbb{Z}$ es una unidad si, y sólo si, m es primo con n. Por $\varphi(n)$ se designa el número de unidades de $\mathbb{Z}/n\mathbb{Z}$, esto es, el número de enteros positivos menores que n y primos

con n. La función φ se denomina *función indicatriz de* EULER (*vid. supra* § 18.4.1 [pág. 983 de esta edición]).

§ 17.12.1 Grupo ordenado

Definición 17.79.— Llamamos *magma ordenado* (resp., *semigrupo ordenado*, *monoide ordenado*, *grupo ordenado*) a la terna $(A; *; \preccurlyeq)$, en la que $\preccurlyeq$ es una relación diádica de orden en A y $(A; *)$ es un magma (resp., semigrupo, monoide o grupo) con $\preccurlyeq$ isótona con $*$.

Ejemplo 500

Siendo $+$, $\cdot$ y $\leq$, la suma, el producto y el orden habituales en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, ¿qué clase de monoides o grupos ordenados son $(\mathbb{N}; +; \leq)$, $(\mathbb{N}; \cdot; \leq)$, $(\mathbb{Z}; +; \leq)$, $(\mathbb{Q}; +; \leq)$ y $(\mathbb{R}; +; \leq)$?

Resolución.— Se satisface:

- $(\mathbb{N}; +; \leq)$ y $(\mathbb{N}; \cdot; \leq)$ son *monoides conmutativos totalmente ordenados* (*vid. supra* teorema 15.11 [pág. 791 de esta edición]);
- $(\mathbb{Z}; +; \leq)$, $(\mathbb{Q}; +; \leq)$ y $(\mathbb{R}; +; \leq)$ son *grupos conmutativos totalmente ordenados*. ■

Observación 17.12.2.— Para ciertos magmas, la propiedad de isotonía se relaja en cierta forma, aunque procurando siempre conservar esta idea de compatibilidad entre la relación de orden y la ley de composición interna. Es el caso, por ejemplo, de los magmas multiplicativos $(\mathbb{Z}; \cdot)$, $(\mathbb{Q}; \cdot)$ y $(\mathbb{R}; \cdot)$, en el que dicha compatibilidad queda reflejada por la exigencia, para el orden habitual $\leq$, de que $\forall a, b, c \in A$, se satisfaga: $a \leq b \wedge c > 0 \rightarrow (c \cdot a \leq c \cdot b) \wedge (a \cdot c \leq b \cdot c)$.
Sin embargo, puede que no se pueda, por ejemplo, para la diferencia en los naturales la situación es distinta, ocurre que si $a \leq b$, entonces $a - c \leq b - c$ (si $c \leq a$) y $c - a \leq c - b$ (si $b \leq c$); suele decirse que la sustracción es *parcialmente isótona*.

Ejemplo 501

Dicho lo anterior y siendo $+$, $\cdot$ y $\leq$, la suma, el producto y el orden habituales en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, ¿qué clase de monoides o grupos ordenados son $(\mathbb{Z}; \cdot; \leq)$, $(\mathbb{Q}\backslash\{0\}; \cdot; \leq)$ y $(\mathbb{R}\backslash\{0\}; \cdot; \leq)$?

Resolución.— Se satisface:

- $(\mathbb{Z}; \cdot; \leq)$ es un *monoide conmutativo totalmente ordenado*;
- $(\mathbb{Q}\backslash\{0\}; \cdot; \leq)$ es un *grupo conmutativo totalmente ordenado*;

- $(\mathbb{R}\backslash\{0\};\cdot;\leq)$ es un *grupo conmutativo totalmente ordenado*. ■

Teorema 17.63

Sean $(G;*;\preccurlyeq)$ un grupo totalmente ordenado y $a,b,c,d\in G$. Se satisface:

	$(G;+;\preccurlyeq)$ (aditivo)		$(G;\cdot;\preccurlyeq)$ (multiplicativo)
0.	$(a\preccurlyeq a)$	0.	$(a\preccurlyeq a)$
1.	$(a\preccurlyeq b)\wedge(b\preccurlyeq a)\to a=b$	1.	$(a\preccurlyeq b)\wedge(b\preccurlyeq a)\to a=b$
2.	$(a\preccurlyeq b)\wedge(b\preccurlyeq c)\to a\preccurlyeq c$	2.	$(a\preccurlyeq b)\wedge(b\preccurlyeq c)\to a\preccurlyeq c$
3.	$(a\preccurlyeq b)\veebar(a=b)\veebar(b\preccurlyeq a)$	3.	$(a\preccurlyeq b)\veebar(a=b)\veebar(b\preccurlyeq a)$
4.	$0\preccurlyeq 1$	4.	$0\preccurlyeq 1$
5.		5.	$a\neq 0\to 0\prec aa$
6.	$a\preccurlyeq b\to(a+c\preccurlyeq b+c)$	6.	$a\preccurlyeq b\wedge c\succ 0\to(ac\preccurlyeq bc)$
7.		7.	$a\preccurlyeq b\wedge c\prec 0\to(bc\preccurlyeq ac)$
8.	$(a\preccurlyeq b)\wedge(c\preccurlyeq d)\to a+c\preccurlyeq b+d$	8.	$(a\preccurlyeq b)\wedge(c\preccurlyeq d)\to ac\preccurlyeq bd$
9.	$a\preccurlyeq b\leftrightarrow -b\preccurlyeq -a$	9.	$a\preccurlyeq b\leftrightarrow b^{-1}\preccurlyeq a^{-1}$

Definición 17.80 (Monoide ordenado arquimediano).— Decimos que un monoide ordenado $(M;*;\preccurlyeq)$ satisface la *propiedad arquimediana* (o simplemente, que es *arquimediano*) si, y sólo si,

$$(\forall q\in M)(\forall p\in M\text{ tal que }e_*\prec p)(\exists n\in\mathbb{Z}^+)(q\prec np),$$

donde $np\fallingdotseq p*\overset{n}{\cdots}*p$.

Definición 17.81 (Grupo ordenado arquimediano).— Decimos que un grupo ordenado $(G;*;\preccurlyeq)$ satisface la *propiedad arquimediana* (o simplemente, que es *arquimediano*) precisamente si la satisface como monoide ordenado, esto es, si, y sólo si,

$$(\forall q\in G)(\forall p\in G\text{ tal que }e_*\prec p)(\exists n\in\mathbb{Z}^+)(q\prec np),$$

donde $np\fallingdotseq p*\overset{n}{\cdots}*p$.

Ejemplo 502

Siendo $+$, $\cdot$ y $\leq$, la suma, el producto y el orden habituales en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, ¿qué clase de magmas ordenados son $(\mathbb{N};+;\leq)$, $(\mathbb{N};\cdot;\leq)$, $(\mathbb{Z};+;\leq)$, $(\mathbb{Z};\cdot;\leq)$, $(\mathbb{Q};+;\leq)$, $(\mathbb{R};+;\leq)$, $(\mathbb{Q}\backslash\{0\};\cdot;\leq)$ y $(\mathbb{R}\backslash\{0\};\cdot;\leq)$?

Resolución.— Se satisface:

- $(\mathbb{N};+;\leq)$ es un *monoide conmutativo totalmente ordenado arquimediano*, esto es, se satisface que $(\forall q\in\mathbb{N})(\forall p\in\mathbb{N}^+)(\exists n\in\mathbb{Z}^+)(q<np)$;

- $(\mathbb{N}; \cdot; \leq)$ es un *monoide conmutativo totalmente ordenado arquimediano*, esto es, se satisface que $(\forall q \in \mathbb{N})(\forall p \in \mathbb{N}^+)(\exists n \in \mathbb{Z}^+)(q < p^n)$;
- $(\mathbb{Z}; +; \leq)$ es un *grupo conmutativo totalmente ordenado arquimediano*, esto es, se satisface que $(\forall q \in \mathbb{Z})(\forall p \in \mathbb{Z}^+)(\exists n \in \mathbb{Z}^+)(q < np)$;
- $(\mathbb{Z}; \cdot; \leq)$ es un *monoide conmutativo totalmente ordenado arquimediano*, esto es, se satisface que $(\forall q \in \mathbb{Z})(\forall p \in \mathbb{Z}^+ \setminus \{1\})(\exists n \in \mathbb{Z}^+)(q < p^n)$;
- $(\mathbb{Q}; +; \leq)$ y $(\mathbb{R}; +; \leq)$ son *grupos conmutativos totalmente ordenados arquimedianos*.
- $(\mathbb{Q}\setminus\{0\}; \cdot; \leq)$ y $(\mathbb{R}\setminus\{0\}; \cdot; \leq)$ son *grupos conmutativos totalmente ordenados arquimedianos*. ■

§ 17.12.2 Anillo ordenado

Definición 17.82 (Primera definición de anillo ordenado).— Llamamos *anillo ordenado* a la cuaterna $(A; \oplus, \otimes; \preccurlyeq)$, donde $(A; \oplus, \otimes)$ es anillo, $\preccurlyeq$ es una relación diádica de orden total en A y $(A; \oplus; \preccurlyeq)$ es grupo ordenado, significando esto la isotonía de $\preccurlyeq$ respecto de $\oplus$, es decir,

$$(\forall x, y, z \in A)(x \preccurlyeq y \to x \oplus z \preccurlyeq y \oplus z).$$

Observación 17.12.3.— En la definición de anillo ordenado, suele exigirse además que $\preccurlyeq$ sea *isótona* respecto de $\otimes$, esto es,

$$(\forall x, y, z \in A)(x \preccurlyeq y \wedge 0 \succ z) \to (x \otimes z \preccurlyeq y \otimes z),$$

y que $\otimes$ sea *conmutativa*.

Una definición alternativa de anillo ordenado es la siguiente. Notemos que en esta forma la relación $\preccurlyeq$ no viene «impuesta» sino que también se define.

Definición 17.83 (Segunda definición de anillo ordenado).— Sea $(A; \oplus, \otimes)$ un anillo. $(A; \oplus, \otimes; \preccurlyeq)$ es un *anillo ordenado* precisamente si $\exists A^+ \subseteq A$ tal que se satisfacen:

0.°, $0 \notin A^+$,

1.°, $(\forall a \in A)(a \in A^+ \vee a = 0 \vee -a \in A^+)$,

2.°, $(\forall a, b \in A^+)(a \oplus b \in A^+ \wedge a \otimes b \in A^+)$.

La relación $\preccurlyeq$ que aparece en la cuaterna, se define, $\forall a, b \in A$:

- $a \prec b \risingdotseq b \oplus (-a) \in A^+$, y se lee «$a$ precede a b»;
- $a \preccurlyeq b \risingdotseq a \prec b \vee a = b$, y se lee «$a$ precede o es igual a b».

Observación 17.12.4.— Frecuentemente se escribe $a \succ b$ en vez de $b \prec a$ y se lee «a sucede a b», y $a \succcurlyeq b$ en vez de $b \preccurlyeq a$ y se lee «a sucede o es igual a b».

Definición 17.84.— Sean $(A; \oplus, \otimes; \preccurlyeq)$ un anillo ordenado y $a \in A$. Decimos que:

- a es *positivo* precisamente si $a \in A^+$;
- a es *negativo* precisamente si $a \neq 0$ y $-a \in A^+$.

El conjunto de los elementos negativos de un anillo ordenado $(A; \oplus, \otimes; \preccurlyeq)$ lo designamos por A^-. No obstante, en la literatura también aparecen los signos más y menos como subíndices: A_+ y A_- en vez de A^+ y A^-, respectivamente.

Teorema 17.64
$A = A^- \cup \{0\} \cup A^+$.

Teorema 17.65 (Propiedades)
Sean $(A; \oplus, \otimes; \preccurlyeq)$ un anillo ordenado y $a, b, c, d \in A$. Se satisface:

0. $a \prec b \wedge b \prec c \rightarrow a \prec c$;
1. $a \neq 0 \rightarrow a \otimes 0 \prec a$;
2. $a \prec b \rightarrow a \oplus c \prec b \oplus c$;
3. $a \prec b \wedge c \prec d \rightarrow a \oplus c \prec b \oplus d$;
4. $0 \prec 1$;
5. $a \prec b \wedge c \succ 0 \rightarrow a \otimes c \prec b \otimes c$;
6. $a \prec b \wedge c \prec 0 \rightarrow b \otimes c \prec a \otimes c$.

Definición 17.85 (Anillo ordenado arquimediano).— Decimos que un anillo ordenado $(A; \oplus, \otimes; \preccurlyeq)$ satisface la *propiedad arquimediana* (o simplemente, que es *arquimediano*) precisamente si el grupo abeliano ordenado $(A; \oplus; \preccurlyeq)$ la satisface, esto es, si, y sólo si,

$$(\forall q \in A)(\forall p \in A^+)(\exists n \in \mathbb{Z}^+)(q \prec n \otimes p).$$

Observación 17.12.5 (Semianillo ordenado arquimediano).— Decimos que un semianillo ordenado $(A; \oplus, \otimes; \preccurlyeq)$ es *arquimediano* precisamente si el monoide abeliano ordenado $(A; \oplus; \preccurlyeq)$ satisface la propiedad arquimediana[26].

[26] *Vid. supra* definición 17.80 (pág. 915 de esta edición).

Ejemplo 503

Siendo $+$, $\cdot$ y $\leq$, la suma, el producto y el orden habituales en $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$, ¿qué clase de semianillos o anillos ordenados son $(\mathbb{N}; +, \cdot; \leq)$, $(\mathbb{Z}; +, \cdot; \leq)$, $(\mathbb{Q}; +, \cdot; \leq)$ y $(\mathbb{R}; +, \cdot; \leq)$?

Resolución.— Se satisface:

- $(\mathbb{N}; +, \cdot; \leq)$ es un semianillo conmutativo, totalmente ordenado, unitario, íntegro y arquimediano;
- $(\mathbb{Z}; +, \cdot; \leq)$, $(\mathbb{Q}; +, \cdot; \leq)$ y $(\mathbb{R}; +, \cdot; \leq)$ son anillos conmutativos, totalmente ordenados, unitarios, íntegros y arquimedianos. ■

Valor absoluto

Definición 17.86.— Sean $(A; \oplus, \otimes; \preccurlyeq)$ un anillo ordenado y $a \in A$. Definimos el *valor absoluto* del elemento a por

$$|a| = \begin{cases} -a & \text{si} \quad a \prec 0 \\ a & \text{si} \quad 0 \prec a \end{cases}$$

Observación 17.12.6.— Asimismo podría definirse el valor absoluto a partir del máximo[27]:

$$|a| = \text{máx}\left(\{a, -a\}, A\right)$$

(aunque también viceversa, el máximo en función del valor absoluto).

Teorema 17.66 (Propiedades del valor absoluto, I)

Sea $(A; \oplus, \otimes; \preccurlyeq)$ un anillo ordenado. Entonces, $\forall a, b \in A$, se satisface:

0. $|a| \succcurlyeq 0$;
1. $|a| = 0 \leftrightarrow a = 0$;
2. $a \preccurlyeq |a|$;
3. $a = b \rightarrow |a| = |b|$;
4. $|a| = |b| \rightarrow a = \pm b$;
5. $a = \pm|a|$;
6. $|a| = |-a|$.

[27] *Vid. infra* definición 11.62 (pág. 654 de esta edición).

Teorema 17.67 (Propiedades del valor absoluto, II)
Sea $(A; \oplus, \otimes; \preccurlyeq)$ un anillo ordenado. Entonces, $\forall n \in \mathbb{Z}^+$, $\forall a, b, a_0, a_1, \ldots, a_n \in A$, se satisface:

7. $|a \otimes b| = |a| \otimes |b|$;
8. $|a_0 \otimes a_1 \otimes \cdots \otimes a_n| = |a_0| \otimes |a_1| \otimes \cdots \otimes |a_n|$;
9. $|a^n| = |a|^n$;
10. $|a \oplus b| \preccurlyeq |a| \oplus |b|$; (desigualdad triangular)
11. $|a \otimes b| \preccurlyeq a^2 \oplus b^2$;
12. $|a| \ominus |b| \preccurlyeq ||a| \ominus |b|| \preccurlyeq |a \ominus b| \preccurlyeq |a| \oplus |b|$.

Teorema 17.68 (Propiedades del valor absoluto, III)
Sea $(A; \oplus, \otimes; \preccurlyeq)$ un anillo ordenado. Entonces, $\forall a, b, c \in A$, con $0 \preccurlyeq b, c$, se satisface:

13. $|a| \preccurlyeq b \leftrightarrow (-b \preccurlyeq a) \wedge (a \preccurlyeq b)$;
14. $b \preccurlyeq |a| \leftrightarrow (a \preccurlyeq -b) \vee (b \preccurlyeq a)$;
15. $|a \ominus b| \preccurlyeq c \leftrightarrow (b \ominus c \preccurlyeq a) \wedge (a \preccurlyeq b \oplus c)$;
16. $c \preccurlyeq |a \ominus b| \leftrightarrow (a \preccurlyeq b \ominus c) \vee (b \oplus c \preccurlyeq a)$;
17. $|a \oplus b| \preccurlyeq c \leftrightarrow (-b \ominus c \preccurlyeq a) \wedge (a \preccurlyeq -b \oplus c)$;
18. $c \preccurlyeq |a \oplus b| \leftrightarrow (a \preccurlyeq -b \ominus c) \vee (-b \oplus c \preccurlyeq a)$.

Ejemplo 504

Dado $b \in \mathbb{Z}$, con $0 \leq b$, ¿cuál es el conjunto de números enteros que satisface $|x| \leq b$?

Resolución.— Según la primera propiedad de la lista de este último teorema, es el conjunto $\{x \in \mathbb{Z} : -b \leq x \leq b\}$, es decir, el intervalo cerrado entero de extremos $-b$ y b, esto es, $[-b, b] \cap \mathbb{Z}$. ∎

Actividad 17.12
Sean $a, b, c, d \in \mathbb{R}$. Exprese en función de intervalos de números reales, la desigualdad $|a - b| \leq |c - d|$.

Elementos destacados

Teorema 17.69 (Caracterización de ínfimo)
Sean $(A; \oplus, \otimes; \preccurlyeq)$ un anillo ordenado, $B \subseteq A$ e $i \in A$. Entonces:

$$i = \text{ínf}(B, A) \leftrightarrow \begin{cases} i \in \text{cinf}(B, A) \\ \wedge \\ (\forall \varepsilon \in A^+)(\exists b \in B)(i \preccurlyeq b \prec i \oplus \varepsilon). \end{cases}$$

Teorema 17.70 (Caracterización de supremo)
Sean $(A; \oplus, \otimes; \preccurlyeq)$ un anillo ordenado, $B \subseteq A$ y $s \in A$. Entonces:

$$s = \sup(B, A) \leftrightarrow \begin{cases} s \in \text{csup}(B, A) \\ \wedge \\ (\forall \varepsilon \in A^+)(\exists b \in B)(s \ominus \varepsilon \prec b \preccurlyeq s). \end{cases}$$

§ 17.12.3 Cuerpo ordenado

Definición 17.87 (Primera definición de cuerpo ordenado).— Un *cuerpo ordenado* es todo cuerpo que como anillo es ordenado, esto es, siendo $(K; \oplus, \otimes)$ un cuerpo y $\preccurlyeq$ una relación de orden total en K, decimos que $(K; \oplus, \otimes; \preccurlyeq)$ es un cuerpo ordenado, precisamente si $\forall x, y, z \in K$ se satisface:

0.°, $x \preccurlyeq y \rightarrow x \oplus z \preccurlyeq y \oplus z$ ($\preccurlyeq$ monótona para $\oplus$);

1.°, $(x \preccurlyeq y \wedge z \in K^+) \rightarrow (x \otimes z \preccurlyeq y \otimes z)$ ($\preccurlyeq$ monótona para $\otimes$).

Observación 17.12.7.— Todo cuerpo ordenado es un anillo ordenado. Precisamente por esto, todo lo visto anteriormente para anillos ordenados es válido para cuerpos ordenados.

Definición 17.88 (Segunda definición de cuerpo ordenado).— Siendo $(K; \oplus, \otimes)$ un cuerpo, definimos la estructura de *cuerpo ordenado* $(K; \oplus, \otimes; \preccurlyeq)$ en la forma alternativa anteriormente descrita para anillo ordenado[28].

Teorema 17.71 (Propiedades)
Sean $(K; \oplus, \otimes; \preccurlyeq)$ un cuerpo ordenado y $a, b \in K$. Se satisface:
0. $a \in K^+ \rightarrow a^{-1} \in K^+$;
1. $0 \prec a \prec b \rightarrow 0 \prec b^{-1} \prec a^{-1}$;
2. $a \prec b \prec 0 \rightarrow b^{-1} \prec a^{-1} \prec 0$.

[28] *Vid. supra* definición 17.83 (pág. 916 de esta edición).

Definición 17.89 (Cuerpo ordenado arquimediano).— Decimos que un cuerpo ordenado $(K; \oplus, \otimes; \preccurlyeq)$ satisface la *propiedad arquimediana* (o simplemente, que es *arquimediano*) precisamente si como anillo ordenado satisface dicha propiedad[29].

Definición 17.90 (Cuerpo ordenado completo).— Decimos que un cuerpo ordenado $(K; \oplus, \otimes; \preccurlyeq)$ es completo precisamente si como conjunto ordenado lo es[30].

Ejemplo 505

Siendo $+, \cdot$ y $\leq$, la suma, el producto y el orden habituales en $\mathbb{Q}$ y $\mathbb{R}$, ¿qué clase de cuerpos ordenados son $(\mathbb{Q}; +, \cdot; \leq)$ y $(\mathbb{R}; +, \cdot; \leq)$?

Resolución.— Se satisface:

- $(\mathbb{Q}; +, \cdot; \leq)$ es cuerpo totalmente ordenado, conmutativo y arquimediano;
- $(\mathbb{R}; +, \cdot; \leq)$ es cuerpo totalmente ordenado, conmutativo, arquimediano y completo. ■

Teorema 17.72

Todo cuerpo ordenado es un cuerpo de característica 0.

Ejemplo 506

Siendo $+, \cdot$ y $\leq$, la suma, el producto y el orden habituales en $\mathbb{Q}$ y $\mathbb{R}$,

- los cuerpos ordenados $(\mathbb{Q}; +, \cdot; \leq)$ y $(\mathbb{R}; +, \cdot; \leq)$ son cuerpos de característica 0 (*vid. supra* ejemplo 497 [pág. 910 de esta edición]).

Valor absoluto en un cuerpo ordenado

Teorema 17.73 (Propiedades)

Sea $(K; \oplus, \otimes; \preccurlyeq)$ un cuerpo ordenado. Entonces, $\forall a \in K, \forall b \in K \setminus \{0\}$, se satisface:

0. $|b^{-1}| = |b|^{-1}$;
1. $|a| \otimes |b|^{-1} = |a \otimes b^{-1}|$;
2. $|a|^2 = a^2$.

[29] *Vid. supra* definición 17.85 (pág. 917 de esta edición).
[30] *Vid. supra* definición 11.68 (pág. 657 de esta edición).

Teorema 17.74 (Desigualdad triangular)
Sea $(K; \oplus, \otimes; \preccurlyeq)$ un cuerpo ordenado. Entonces, $\forall n \in \mathbb{Z}^+$, $\forall i \in [n]$, $\forall a_i, b_i \in K$, se satisface (*vid. supra* apartado 10 del teorema 17.67 [pág. 919 de esta edición])

$$\left| \bigoplus_{i=1}^{n} a_i \right| \leq \bigoplus_{i=1}^{n} |a_i| \, .$$

Teorema 17.75 (Desigualdad de Cauchy-Schwartz)
Sea $(\mathbb{R}; +, \cdot; \leq)$ con $+$, $\cdot$ y $\leq$, la suma, el producto y el orden habituales. Entonces, $\forall n \in \mathbb{Z}^+$, $\forall i \in [n]$, $\forall a_i, b_i \in \mathbb{R}$, se satisface:

$$\left| \sum_{i=1}^{n} a_i b_i \right|^2 \leq \left(\sum_{i=1}^{n} |a_i|^2 \right) \cdot \left(\sum_{i=1}^{n} |b_i|^2 \right) .$$

La igualdad se satisface precisamente si:

$$a_1 \cdot b_1^{-1} = a_2 \cdot b_2^{-1} = \cdots = a_n \cdot b_n^{-1} .$$

Teorema 17.76 (Desigualdad de Hölder)
Sea $(\mathbb{R}; +, \cdot; \leq)$ con $+$, $\cdot$ y $\leq$, la suma, el producto y el orden habituales. Entonces, $\forall n \in \mathbb{Z}^+$, $\forall i \in [n]$, $\forall a_i, b_i \in \mathbb{R}$, $\forall p, q \in (1, +\infty)$, tal que $1/p + 1/q = 1$, se satisface:

$$\left| \sum_{i=1}^{n} a_i b_i \right| \leq \left(\sum_{i=1}^{n} |a_i|^p \right)^{1/p} \cdot \left(\sum_{i=1}^{n} |b_i|^q \right)^{1/q} .$$

La igualdad se satisface precisamente si:

$$|a_1|^{p-1} \cdot |b_1|^{-1} = |a_2|^{p-1} \cdot |b_2|^{-1} = \cdots = |a_n|^{p-1} \cdot |b_n|^{-1} .$$

Si $p = q = 2$, se tiene la desigualdad de Cauchy-Schwartz.

§ 17.12.4 Retículos

Definición 17.91.— Sean S un conjunto no vacío y $*$ una operación en S. Decimos que $(S; *)$ es un *semirretículo* precisamente si es un semigrupo abeliano e idempotente, esto es, si, y sólo si, $*$ es asociativa, conmutativa e idempotente en S, es decir, si, y sólo si,

$$\begin{aligned} (x * y) * z &= x * (y * z) && \text{(asociativa)} \\ x * y &= y * x && \text{(conmutativa)} \\ x * x &= x && \text{(idempotente)} \end{aligned}$$

En todo semirretículo $(S;*)$ es posible definir dos relaciones duales de orden parcial en S:

$$x \leq y \leftrightarrow x * y = x,$$
$$x \geq y \leftrightarrow x * y = y,$$

y recíprocamente, dadas dos relaciones duales de orden parcial en S, es posible definir dos operaciones en S:

$$x \sqcap y = x \leftrightarrow x \leq y,$$
$$x \sqcup y = y \leftrightarrow x \geq y.$$

Es por esto por lo que se distinguen dos tipos duales de semirretículos, denominados semirretículo inferior $(S;\sqcap)$ y semirretículo superior $(S;\sqcup)$. A estas operaciones $\sqcap$ y $\sqcup$ se les conoce como ínfimo y supremo, respectivamente.

Observación 17.12.8.— Lo expuesto puede igualmente comenzarse desde la teoría del orden: $(L,\sqcup)$ es un semirretículo inferior precisamente si es un conjunto parcialmente ordenado en el que existe un ínfimo para todo subconjunto no vacío finito y $(L,\sqcap)$ es un semirretículo superior precisamente si es un conjunto parcialmente ordenado en el que existe un supremo para todo subconjunto no vacío finito.

Ejemplo 507

Todo árbol enraizado es un semirretículo inferior.

Definición 17.92.— Sean un conjunto $L \neq \emptyset$ y $\sqcap, \sqcup : L \times L \longrightarrow L$ dos operaciones diádicas definidas en L. Decimos que $(L;\sqcap,\sqcup)$ es un *retículo* precisamente si —*cfr.* BIRKHOFF [193]; GRÄTZER [194]— $(L;\sqcap)$ es un semigrupo abeliano, $(L;\sqcup)$ es un semigrupo abeliano y se satisfacen las leyes de absorción (a veces llamadas también de simplificación), esto es, si, y sólo si, las operaciones $\sqcap$ (*meet*) y $\sqcup$ (*join*) satisfacen:

0.°, $(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$ y $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$ (asociativas),

1.°, $x \sqcap y = y \sqcap x$ y $x \sqcup y = y \sqcup x$ (conmutativas),

2.°, $x \sqcap (x \sqcup y) = x$ y $x \sqcup (x \sqcap y) = x$ (leyes de absorción).

Precisamente son estas dos últimas, las identidades de absorción, las que muestran la interacción de los dos semirretículos $(L;\sqcap)$ y $(L;\sqcup)$ en una entidad mayor, el retículo. Observemos que en la definición de retículo no se exigen las idempotencias de $\sqcap$ y $\sqcup$ en L y esto se debe a que se deducen de las demás exigencias.

Observación 17.12.9.— Jean DESANTI [195] —*via* Jesús IBÁÑEZ (coord.) [196] (pág. 96)— apunta el uso de otras denominaciones en la literatura: *rejilla*, *enrejado* (*treillis*), *estructuras* (Øystein ORE y Valery Ivanovich GLIVENKO) y *Systeme von Dingen* (Karl MENGER). También, aunque antes con mayor frecuencia, aparece traducido como «laticia» (del inglés *lattice*) o *retícula*.

Teorema 17.77
Si $(L; \sqcap, \sqcup)$ es un retículo, entonces $(L, \preceq)$ es un conjunto parcialmente ordenado, donde $x \preceq y \leftrightharpoons x \sqcap y = x$.

Teorema 17.78
Si $(L, \preceq)$ es un conjunto parcialmente ordenado y se definen $x \sqcap y \leftrightharpoons \inf\{x, y\}$ y $x \sqcup y \leftrightharpoons \sup\{x, y\}$, entonces, el magma $(L; \sqcap, \sqcup)$ es un retículo.

De estos dos últimos teoremas se sigue de inmediato el siguiente.

Teorema 17.79
Un conjunto ordenado parcialmente $(L, \preceq)$ es un retículo precisamente si todo subconjunto formado por dos elementos tiene ínfimo y supremo en L.

Observación 17.12.10.— En algunos textos aparece como definición de retículo lo afirmado por el teorema anterior (o, si acaso, en vez de dos elementos, un número finito de elementos), por ejemplo así: Decimos que un conjunto ordenado $(L, \preceq)$ es un retículo si, y sólo si, todo subconjunto de dos elementos de L tiene supremo e ínfimo.

Ejemplo 508

Sea un conjunto $L \neq \emptyset$; se tiene que $(2^L; \subseteq)$ es un retículo.

Resolución.— En efecto, cualquier subconjunto de dos elementos $\{A, B\}$ tiene ínfimo y supremo, $A \cap B$ y $A \cup B$, respectivamente. Notemos que esto equivale a definir las operaciones $\sqcap = \cap$ y $\sqcup = \cup$. ■

Actividad 17.13

Demostremos que $(\mathbb{N}; |)$ es un retículo ($|$ denota la relación de divisibilidad).
Sugerencia.— Definamos $x \sqcap y = \mathrm{mcd}(x, y)$ y $x \sqcup y = \mathrm{mcm}(x, y)$.
Observación.— Las operaciones mcm y mcd en $(\mathbb{N}; |)$ se comportan, respectivamente, como $\cup$ y $\cap$ en $(2^L; \subseteq)$ del ejemplo anterior.

Actividad 17.14

El conjunto de todas las particiones de un conjunto de cardinal n con la relación de dominancia (una partición domina a otra si, y sólo si, es más fina), ¿tiene estructura de retículo?

Teorema 17.80 (De inducción de reticulado)
Dados $(A, \leq)$ un retículo y $(B, \subseteq)$ un conjunto ordenado, se satisface que si $f : A \longrightarrow B$ es un isomorfismo entre conjuntos ordenados, entonces $(B, \subseteq)$ es un retículo.

§ 17.12.5 Álgebra de Boole

Ya estudiamos en § 3.7 (pág. 353 de esta edición) la estructura de álgebra de Boole y mostramos allí y a lo largo de los epígrafes siguientes varios ejemplos.

Ejemplo 509 (Algunos modelos de álgebras de Boole)

0. $(\{F, V\}, \vee, \wedge, \neg)$ es el *álgebra de* Boole *de la lógica de juntores*.
1. El *álgebra de conmutación* $(\{0, 1\}; +, \cdot, ')$ del análisis de circuitos electrónicos es un álgebra de Boole.
2. El *álgebra de de los conjuntos*: dado un conjunto referencial finito U, la cuaterna $(2^U; \cup, \cap, ^{\complement})$ tiene estructura de álgebra de Boole.

Ahora, tras estudiar los retículos, proporcionamos una nueva definición de álgebra de Boole.

Definición 17.93.— Un *álgebra de* Boole (o, sinónimamente, *retículo de* Boole) es todo retículo distributivo y complementado.

Definición 17.94.— Sean $(X; \sqcup, \sqcap, ')$ y $(Y; \triangle, \triangledown, ^{\perp})$ dos álgebras de Boole y $f : X \longrightarrow Y$ una aplicación. Decimos que f es un *homomorfismo de álgebras de* Boole precisamente si para cualesquiera elementos x, y de X se satisface:

0.°, $f(x \sqcup y) = f(x) \triangle f(y)$,

1.°, $f(x \sqcap y) = f(x) \triangledown f(y)$,

2.°, $f(0_X) = 0_Y$,

3.°, $f(1_X) = 1_Y$.

Teorema 17.81

Sean $(X; \sqcup, \sqcap, ')$ y $(Y; \triangle, \triangledown, ^{\perp})$ dos álgebras de BOOLE y $f : X \longrightarrow Y$ un homomorfismo entre ellas. Se satisface que $\forall x \in X, f(x') = f(x)^{\perp}$.

§ 17.13 Otras estructuras de interés

§ 17.13.0 Álgebra de conjuntos

Un *álgebra* sobre un conjunto X es un conjunto no vacío C de subconjuntos de X, tal que el conjunto vacío es elemento de C y éste es cerrado con respecto a las operaciones unión finita, intersección y complemento relativo a X, o lo que es equivalente, si, y sólo si, C es un subconjunto de 2^X tal que

0.°, $\emptyset \in C$ (o equivalentemente, $X \in C$),

1.°, $C \setminus S \in C$, para todo $S \in C$,

2.°, $S \cup T \in C$, para todo $S, T \in C$.

Llamamos *álgebra de conjuntos* al par ordenado $\langle X, C \rangle$ (también se conoce como *álgebra de* BOOLE *concreta*).

Si una álgebra sobre un conjunto X es cerrada para la unión infinita numerable (y por tanto para la intersección infinita numerable), decimos que es una *sigma álgebra* sobre X. La álgebra de conjuntos asociada se denomina *espacio medible*. Un *espacio de medida* es una tripleta $\langle X, C, \mu \rangle$, donde $\langle X, C \rangle$ es un espacio medible y μ es una *medida* definida en él. Si μ es una *medida de probabilidad*, decimos que el espacio medible subyacente es un *espacio muestral*.

Ejemplo 510 (Algunos modelos de σ-álgebras)

Si X es un conjunto, entonces:

0. el conjunto $\{\emptyset, X\}$ es la que se denomina *σ-álgebra minimal* (o, sinónimamente, *σ-álgebra trivial*) sobre X;
1. el conjunto potencia de X es la que se conoce como la *σ-álgebra discreta* sobre X;
2. el conjunto $\{\emptyset, A, A^{\complement}, X\}$ es la *σ-álgebra más simple* sobre X generada por A;
3. el conjunto de subconjuntos vacíos, finitos o numerables o cuyos complementos son vacíos, finitos o numerables (que es distinto del conjunto potencia de X si, y sólo si, X es infinito no numerable) es una *σ-álgebra generada por los subconjuntos unitarios* de X;
4. dada una partición finita o numerable P de X, el conjunto de todas las uniones de elementos de P es una σ-álgebra sobre X.

Teorema 17.82
Toda álgebra de conjuntos es un álgebra de BOOLE, pero no toda álgebra de BOOLE es un álgebra de conjuntos.

§ 17.13.1 Anillo de BOOLE

Definición 17.95.— Un *anillo de* BOOLE es un anillo unitario $(X; \boxplus, \boxtimes)$ tal que todos sus elementos son idempotentes, esto es, tal que $\forall x \in X, x \boxtimes x = x$.

Es posible definir un anillo de BOOLE a partir de un álgebra de BOOLE.

Teorema 17.83
Si $(X; \sqcap, \sqcup, ')$ es un álgebra de BOOLE, entonces X con las operaciones $\boxplus$ y $\boxtimes$ definidas, para todo x, y de X, por

$$x \boxplus y = (x \sqcap y') \sqcup (x' \sqcap y),$$
$$x \boxtimes y = x \sqcap y,$$

tiene estructura de anillo de BOOLE, siendo el neutro multiplicativo el 1 del álgebra de BOOLE. Decimos que $(X; \boxplus, \boxtimes)$ es el *anillo de* BOOLE *asociado* al álgebra de BOOLE $(X; \sqcap, \sqcup, ')$.

Recíprocamente, puede definirse un álgebra de BOOLE a partir de un anillo de BOOLE.

Teorema 17.84
Si $(X; \boxplus, \boxtimes)$ es un anillo de BOOLE, entonces X con las operaciones $\sqcap, \sqcup$ y $'$ definidas, para todo x, y de X, por

$$x \sqcap y = x \boxtimes y,$$
$$x \sqcup y = x \boxplus y \boxplus (x \boxtimes y),$$
$$x' = 1 \boxplus x,$$

tiene estructura de álgebra de BOOLE. Decimos que $(X; \sqcap, \sqcup, ')$ es el *álgebra de* BOOLE *asociada* al anillo de BOOLE $(X; \boxplus, \boxtimes)$.

§ 17.13.2 Espacio vectorial

Definición 17.96.— Un *espacio vectorial sobre un cuerpo* K es un conjunto V junto a una ley de composición interna (suma) y una ley de composición externa (producto por un escalar del cuerpo), tales que $(V; +)$ es grupo abeliano y la ley de composición externa $K \times V \longrightarrow V, (\lambda, v) \mapsto \lambda v$, es tal que

$\lambda(u+v) = \lambda u + \lambda v)$, $(\lambda+\mu)v = \lambda v + \mu v$, $\lambda(\mu v) = (\lambda\mu)v$ y $1v = v$ para cualesquiera $u, v \in V$ y $\lambda, \mu \in K$.

Definición 17.97.— Un *subespacio vectorial* es un subconjunto U de un espacio vectorial V que es espacio vectorial con las restricciones a U de las leyes de composición de V

Teorema 17.85
U es subespacio vectorial si, y sólo si, $U \neq \emptyset$ y $\forall u, v \in U, \forall \lambda, \mu \in K, \lambda u + \mu v \in U$.

Teorema 17.86
La unión de subespacios vectoriales es subespacio vectorial mientras que la intersección no tiene por qué serlo.

Ejemplo 511

Pensemos en las funciones escalonadas definidas en $[a, b]$ respecto de una misma partición $\{[x_0, x_1], (x_1, x2], \ldots, (x_{n-1}, x_n]\}$ de $[a, b]$ (siendo $x_0 = a$ y $x_n = b$); ¿con respecto a qué operaciones es un espacio vectorial?.

Resolución.— Con respecto a la suma habitual de funciones y el producto de funciones por un número real; se trata de $(\mathcal{E}([a, b]); +, \cdot)$, el *espacio vectorial de las funciones escalonadas* definidas en la forma dicha en el enunciado. ■

Observación 17.13.0.— Las funciones escalonadas son interesantes porque, por un lado, tratan de lo discreto, son constantes a trozos, siendo cierto, por ejemplo, que toda función continua puede aproximarse por funciones escalonadas y, por otro, porque intervienen en hechos cotidianos como en los procesos recaudatorios, sean impuestos o voluntarios por donación.

¡Un saludo, tata ... tatarabuelo robot![*]

No en vano provenimos de autómatas[†].

Aquellas macromoléculas[‡] de hace miles de millones de años, de las que descendemos[§], no eran más que eso, autómatas[¶] autoduplicantes[×].

Y son nuestros ancestros.

---

[*] Esta expresión tan gráfica es de Daniel Clement DENNETT y aparece en su libro *Tipos de Mentes*, ed. Debate, Madrid, 2000, pág. 34 (trad. de Francisco Páez de la Cadena, de *Kinds of Minds*, 1996).

[†] Leamos sobre la *teoría de autómatas*, también conocida como *teoría algebraica de las máquinas* (*cfr. v. gr.* https://en.wikipedia.org/wiki/Automata_theory).

[‡] *Vid. v. gr.* https://en.wikipedia.org/wiki/Macromolecule.

[§] *Vid. v. gr.* https://en.wikipedia.org/wiki/Outline_of_evolution.

[¶] *Vid. v. gr.* https://link.springer.com/chapter/10.1007/978-3-540-87531-4_4.

× *Vid. v. gr.* https://en.wikipedia.org/wiki/Self-replication.

§ 17.14 Acerca de algunas cuestiones y conjeturas famosas

Sobre algunas cuestiones abiertas y algunas afirmaciones o negaciones aún no demostradas ni refutadas.

- Conjetura Köthe (1930) (*cfr. v. gr.* https://en.wikipedia.org/wiki/K%C3%B6the_conjecture).
- Conjetura divisor de cero de Kaplansky (*cfr. v. gr.* https://en.wikipedia.org/wiki/Kaplansky%27s_conjectures#Group_rings).
- Conjetura idempotente de Kaplansky (*cfr. v. gr.* https://en.wikipedia.org/wiki/Kaplansky%27s_conjectures#Group_rings).
- Conjetura unidad de Kaplansky (*cfr. v. gr.* https://en.wikipedia.org/wiki/Kaplansky%27s_conjectures#Group_rings).

§ 17.15 Algunas conjeturas que se han convertido en teoremas

Teorema 17.87 (Teorema de Frobenius)
Cfr. v. gr. https://en.wikipedia.org/wiki/Frobenius%27s_theorem_(group_theory).

§ 17.16 Muestra de más ejemplos

Ejemplo 512

Sea $\boxtimes$ la ley de composición diádica definida en $A = \{1, 3, 5, 7, 9\}$ por $(\forall x, y \in A)(x \boxtimes y = u)$, donde u es la cifra de las unidades del producto habitual $x \times y$ entre números naturales —por ejemplo, $3 \boxtimes 9 = 7$—.

0. Hallemos razonadamente la tabla de Cayley de $\boxtimes$ en A.
1. Estudiemos si $(A; \boxtimes)$ tiene estructura de: I, magma; II, semigrupo; III, monoide; IV, grupo.
2. Hallemos razonadamente un subconjunto S de A tal que $(S; \boxtimes)$ sea un grupo de orden cuatro.
3. ¿A cuál es isomorfo $(S; \boxtimes)$, al grupo cíclico C_4 o al grupo de Klein K_4? ¿Por qué?

ⓘ Para responder a los apartados II, III y IV, es aceptable razonar con la tabla hallada en I.

[EFE 22.6.2022:4], [EFE 19.1.2023:4], [EFO 24.5.2023:4], [SEL 5:4]. *Cfr.* Anzola y Caruncho [140]: problema 10.20 (pág. 216).

Resolución.—

0. De acuerdo a la definición de la ley de composición $\boxtimes$ y a la construcción

$$\begin{array}{c|ccc} \boxtimes & \dots & j & \dots \\ \hline \vdots & \dots & \vdots & \dots \\ i & \dots & i \boxtimes j & \dots \\ \vdots & \dots & \vdots & \dots \end{array}$$

la tabla de Cayley de $\boxtimes$ en A es

$\boxtimes$	1	3	5	7	9
1	1	3	5	7	9
3	3	9	5	1	7
5	5	5	5	5	5
7	7	1	5	9	3
9	9	7	5	3	1

Observemos que la tabla es en realidad la del producto habitual de números naturales, sólo que hemos ocultado las cifras de las decenas:

$\boxtimes$	1	3	5	7	9
1	1	3	5	7	9
3	3	9	15	21	27
5	5	15	25	35	45
7	7	21	35	49	63
9	9	27	45	63	81

1.

I. $(A;\boxtimes)$ *tiene estructura de magma*. En efecto, la ley de composición $\boxtimes$ es una operación en A ya que, como puede verse en la tabla de Cayley, todos los resultados son elementos de A. Además, el hecho de ser la tabla de Cayley simétrica demuestra que $\boxtimes$ es conmutativa en A —de hecho, lo es por serlo el producto de números naturales—. En otras palabras, $(A;\boxtimes)$ es un magma abeliano.

II. $(A;\boxtimes)$ *tiene estructura de semigrupo*, en realidad de semigrupo abeliano al ser $\boxtimes$ conmutativa en A. Como hemos demostrado ya que tiene estructura de magma, sólo necesitamos demostrar que $\boxtimes$ es asociativa en A. En efecto, así es, por serlo el producto de números naturales.

III. $(A;\boxtimes)$ *tiene estructura de monoide*, en realidad de monoide abeliano al ser $\boxtimes$ conmutativa en A. Como hemos demostrado ya que tiene estructura de semigrupo, sólo necesitamos demostrar que existe el elemento neutro en A para $\boxtimes$. En efecto, el elemento neutro de $\boxtimes$ en A es 1 por ser éste el neutro del producto de números naturales. Alternativamente, pudiésemos observar la tabla de Cayley: la primera fila es copia literal de la fila de cabecera, esto es, $(\forall y \in A)(1 \boxtimes y = y)$, es decir, 1 es el neutro por la izquierda de $\boxtimes$ en A; análogamente, la primera columna es copia literal de la columna de cabecera, esto es, $(\forall x \in A)(x \boxtimes 1 = x)$, es decir, 1 es el neutro por la derecha de $\boxtimes$ en A. Al ser 1 el neutro por la izquierda y por la derecha de $\boxtimes$ en A, es el neutro de $\boxtimes$ en A (si bien por ser $\boxtimes$ conmutativa en A bastaba demostrarlo por un lado).

IV. $(A;\boxtimes)$ *no tiene estructura de grupo* por no ser todos sus elementos simetrizables. En efecto, existe un elemento no simetrizable en $(A;\boxtimes)$, a saber, 5, lo que se demuestra con la tabla de Cayley al no aparecer el neutro en la fila correspondiente a 5, por lo que no existe $y \in A$ tal que $5 \boxtimes y = 1$, esto es, no existe simétrico por la derecha de 5 en A; análogamente, no existe $x \in A$ tal que $x \boxtimes 5 = 1$, es decir, no existe simétrico por la izquierda de 5 en A. Con la tabla de Cayley se demuestra que el resto de elementos de A sí son simetrizables respecto de $\boxtimes$ en A:

$$1 \boxtimes 1 = 1 \to 1^{-1} = 1,$$

$$3 \boxtimes 7 = 7 \boxtimes 3 = 1 \rightarrow 7^{-1} = 3,$$
$$7 \boxtimes 3 = 3 \boxtimes 7 = 1 \rightarrow 3^{-1} = 7,$$
$$9 \boxtimes 9 = 1 \rightarrow 9^{-1} = 9.$$

Conclusión.— De I, II y III se sigue que $(A; \boxtimes)$ tiene estructura de monoide abeliano y de IV, que no es grupo.

2. Como hemos demostrado anteriormente, el único elemento no simetrizable es 5, de este modo, el subconjunto de A, $S = \{1, 3, 7, 9\}$ es un grupo con la operación $\boxtimes$; la tabla de CAYLEY de $\boxtimes$ en S es

$\boxtimes$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

El orden de un grupo finito es su número de elementos, luego $(S; \boxtimes)$ es de orden 4.

3. Únicamente existen dos grupos no isomorfos de orden 4, el cíclico C_4 —siendo un ejemplo de modelo suyo el grupo $(\mathbb{Z}_4; +_4)$— y el de KLEIN K_4 —siendo un ejemplo de modelo suyo el grupo, con la operación composición, de las isometrías planas que dejan fijo el rectángulo no cuadrado—.

$C_4 =$

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$K_4 =$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Como $(S; \boxtimes)$ es de orden 4, o bien es isomorfo a C_4 o bien es isomorfo a K_4.

Veamos ahora a cuál. Estudiémoslo de dos formas alternativas.

De una.

Observamos que todos los elementos de K_4 tienen orden 2, esto es, todos los elementos son su propio simétrico—los grupos que satisfacen ésto se denominan *grupos booleanos*[31]—. Resulta que como esto no sucede en $(S; \boxtimes)$, no queda más posibilidad que $(S; \boxtimes)$ sea isomorfo a C_4.

De otra.

Reescribiendo la tabla de $(S; \boxtimes)$, vemos que es isomorfo al grupo cíclico de orden cuatro, C_4.

[31] *Vid. v. gr.* https://en.wikipedia.org/wiki/Elementary_abelian_group.

$$C_4 = \begin{array}{c|cccc} & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & b & c & e \\ b & b & c & e & a \\ c & c & e & a & b \end{array} \qquad (S;\boxtimes) = \begin{array}{c|cccc} & 1 & 3 & 9 & 7 \\ \hline 1 & 1 & 3 & 9 & 7 \\ 3 & 3 & 9 & 7 & 1 \\ 9 & 9 & 7 & 1 & 3 \\ 7 & 7 & 1 & 3 & 9 \end{array}$$

Observación 17.16.0.— Particularmente, C_4 está engendrado por a, esto es, sus elementos son a, $a^2 = b$, $a^3 = c$, $a^4 = e$. Por su parte, $(S;\boxtimes)$ está engendrado por 3; en efecto, sus elementos son 3, $3^2 = 9$, $3^3 = 7$, $3^4 = 1$. ■

§ 17.17 Propuesta de más actividades

Actividad 17.15

Sea $(G;*)$ un grupo y $a, b \in G$. Calculemos el inverso de $a * b$.

[EFEC 25.6.2019:2b1].

Actividad 17.16

Demuestre que si en un grupo, cualquier elemento es su propio inverso, entonces el grupo debe ser abeliano.

[EFEC 25.6.2019:2b2].

Actividad 17.17

Sea C un conjunto. Consideremos la diferencia simétrica de conjuntos definida en su conjunto potencia, 2^C:

$$\forall A, B \in 2^C,\ A \oplus B = (A \setminus B) \cup (B \setminus A).$$

Demostremos que $(2^C;\oplus)$ es un grupo abeliano.

[SEL 5:3]. *Cfr.* Anzola y Caruncho [140]: problema 10.29 (pág. 225).

Actividad 17.18

En el conjunto $A = \{0, 1, 2\}$, sea la ley de composición diádica: $\forall x, y \in A, x * y = x + y - x \cdot y$, siendo $+, -$ y $\cdot$ la suma, la diferencia y el producto habituales en $\mathbb{N}$.

0. ¿Es $(A;*)$ un semigrupo abeliano?
1. ¿Es $(A;*)$ un grupo abeliano?

[AIC 10.4.2018:3A].

Actividad 17.19

En el conjunto $A = \{0, 2, 4, 6, 8\}$, consideremos las leyes de composición diádicas definidas por: $\forall x, y \in A, x \boxplus y = u$ siendo u la cifra de las unidades de la suma habitual $x + y$ entre números naturales (por ejemplo, $6 \boxplus 8 = 4$) y $x \boxtimes y = u$ siendo u la cifra de las unidades del producto habitual $x \times y$ entre números naturales (por ejemplo, $6 \boxtimes 8 = 8$).

0. Hallemos las tablas de CAYLEY de $\boxplus$ y $\boxtimes$ en A.
1. ¿Es $(A; \boxplus, \boxtimes)$ un cuerpo conmutativo? (Es aceptable razonar utilizando las tablas de las operaciones en A).
2. Si $(A; \boxplus)$ resultó ser un grupo, será cíclico, ¿verdad?, ¿por qué? ¿Cuál es su generador?
3. En el apartado 1 habremos hallado razonadamente un subconjunto S de A tal que $(S; \boxtimes)$ es un grupo de orden cuatro, ¿a cuál es isomorfo $(S; \boxtimes)$, al grupo cíclico C_4 o al grupo de KLEIN K_4? ¿Por qué? Caso de que lo sea a C_4, ¿cuál es el generador?

[SEL 5:5]. *Cfr.* ANZOLA y CARUNCHO [197]: problema 4.4 (pág. 83).

Actividad 17.20

En el conjunto $A = \{0, -1, -2\}$, sea la ley de composición diádica: $\forall x, y \in A, x \circ y = x + y + x \cdot y$, siendo $+$ y $\cdot$ la suma y el producto habituales en $\mathbb{N}$.

0. ¿Es $(A; \circ)$ un semigrupo abeliano?
1. ¿Es $(A; \circ)$ un grupo abeliano?

[AIC 10.4.2018:3B].

Observación 17.17.0.— Si $(R; +, \cdot)$ es un anillo, unitario o no, la ley de composición $x \circ y = x + y + xy$, para todo $x, y \in R$ es conocida como la multiplicación círculo o *multiplicación adjunta del anillo* R. Se sabe que $((R; +, \cdot); \circ)$ es un monoide (cuyo elemento neutro es 0, el elemento neutro de $+$), monoide conocido como el *semigrupo adjunto del anillo* R. Esta multiplicación círculo satisface las *leyes distributivas generalizadas*, $\forall x, y, z, t \in R$:

$$x \circ (y + z - t) = x \circ y + x \circ z - x \circ t,$$
$$(y + z - t) \circ x = y \circ x + z \circ x - t \circ x,$$

o equivalentemente, $\forall x, y, z \in R$:

$$x \circ (y + z) + x \circ 0 = x \circ y + x \circ z,$$
$$(y + z) \circ x + 0 \circ x = y \circ x + z \circ x.$$

La estructura $(R; +, \diamond)$, donde $(R; +)$ es el grupo abeliano del anillo y $\diamond$ es una operación multiplicativa (asociativa o no) que satisface estas leyes distributivas generalizadas, ha recibido varios nombres en la literatura[32]: *pseudoanillo*, *anillo débil*, *cuasianillo*, *preanillo*.

Actividad 17.21

Sea el conjunto $A = \{0, 1\}$ de los dos únicos valores de verdad en la lógica bivalente de enunciados. Consideremos los juntores $\neg$, $\wedge$, $\vee$, $\veebar$, $\rightarrow$ y $\leftrightarrow$. Estudiemos las siguientes estructuras algebraicas: $(A; \neg)$, $(A; \wedge)$, $(A; \vee)$, $(A; \veebar)$, $(A; \rightarrow)$, $(A; \leftrightarrow)$ y $(A; \veebar, \leftrightarrow)$.

[SEL 5:6].

Observación 17.17.1.— La operación $\leftrightarrow$ definida en el grupo abeliano $(A; \veebar)$ satisface las leyes distributivas generalizadas —*vid. supra* observación 17.17.0 (pág. 934 de esta edición)—, $\forall p, q, r \in A$:

$$(p \leftrightarrow (q \veebar r)) \veebar (p \leftrightarrow 0) \dashv\vdash (p \leftrightarrow q) \veebar (p \leftrightarrow r),$$
$$((q \veebar r) \leftrightarrow p) \veebar (0 \leftrightarrow p) \dashv\vdash (q \leftrightarrow p) \veebar (r \leftrightarrow p).$$

Observación 17.17.2.— Los juntores $\veebar$ y $\leftrightarrow$, además de ser asociativos, son *mutuamente asociativos*; esto permite, por ejemplo, escribir $p \veebar q \leftrightarrow \neg(p \leftrightarrow q)$, sin necesidad de especificar si se trata de $(p \veebar q) \leftrightarrow \neg(p \leftrightarrow q)$ o de $p \veebar (q \leftrightarrow \neg(p \leftrightarrow q))$.

Actividad 17.22

En un triángulo equilátero, el baricentro, el circuncentro, el incentro y el ortocentro coinciden en un mismo punto O y las medianas, las mediatrices, las bisectrices y las alturas, también son las mismas. Sea M el conjunto de los movimientos del plano que dejan invariable al triángulo equilátero (dejan invariable su «forma» pero pueden reorganizar sus vértices): la identidad I, el giro G_1 de centro O y ángulo 120°, el giro G_2 de centro O y ángulo 240° y las simetrías axiales, S_1, S_2 y S_3, de ejes respectivos cada una de las bisectrices. Demostremos que $(M; I, G_1, G_2, S_1, S_2, S_3)$ es un grupo no abeliano.

[SEL 5:7]. *Cfr.* Anzola y Caruncho [140]: problema 10.43 (pág. 235).

Actividad 17.23

Imaginemos cuatro danzantes, originalmente distribuidos en las esquinas de un cuadrado y consideremos los movimientos coreográficos: $I \leftrightharpoons$ permanece cada uno en su sitio —gráficamente: $\begin{vmatrix} \bullet & \bullet \\ \bullet & \bullet \end{vmatrix}$—; $J \leftrightharpoons$ se intercambian los de cada lado horizontal —gráficamente:

[32] *Cfr. v. gr.* Xiankun Du y Junlin Wang, 2006, Generalized Adjoint Semigroups of a Ring, *Contributions to Algebra and Geometry* 47(1), págs. 211–228, disponible en https://www.emis.de/journals/BAG/vol.47/no.1/b47h1du1.pdf.

$\begin{vmatrix} \rightarrow & \leftarrow \\ \rightarrow & \leftarrow \end{vmatrix}$—; $K \leftrightharpoons$ se intercambian los de cada lado vertical —gráficamente: $\begin{vmatrix} \downarrow & \downarrow \\ \uparrow & \uparrow \end{vmatrix}$—; $L \leftrightharpoons$ se intercambian los las esquinas opuestas —gráficamente: $\begin{vmatrix} \searrow & \swarrow \\ \nearrow & \nwarrow \end{vmatrix}$—. Notemos por $*$ la composición de estos movimientos. ¿Qué estructura tiene el conjunto de movimientos $\{I, J, K, L\}$ con dicha operación composición $*$?

Actividad 17.24

Sean las operaciones $\oplus$ y $\otimes$ definidas en $\mathbb{Z} \times \mathbb{Z}$ por, $\forall \langle x, y \rangle, \langle u, v \rangle \in \mathbb{Z} \times \mathbb{Z}$,

$$\langle x, y \rangle \oplus \langle u, v \rangle = \langle x + u, y + v \rangle,$$
$$\langle x, y \rangle \otimes \langle u, v \rangle = \langle xu, xv + yu \rangle.$$

0. Demostremos que $(\mathbb{Z} \times \mathbb{Z}; \oplus, \otimes)$ es un anillo conmutativo unitario.
1. ¿Es $(\mathbb{Z} \times \mathbb{Z}; \oplus, \otimes)$ un dominio de integridad?

[PEP 14.4.2023:4]. *Cfr.* Anzola y Caruncho [197]: problema 1.32 (pág. 26).

Actividad 17.25

Sea $(A; \oplus, \otimes; \lhd)$ un anillo ordenado y $(B; \boxplus, \boxtimes)$ un anillo; sea $f : (B; \boxplus, \boxtimes) \longrightarrow (A; \oplus, \otimes)$ un homomorfismo de anillos. Se define en B la siguiente ley de composición diádica:

$$\forall x, y \in B,\ x \blacktriangleleft y \leftrightarrow f(x) \lhd f(y).$$

0. Demostremos que $\blacktriangleleft$ no es en general una relación de orden en B.
1. 0.a. ¿Qué debe satisfacer f para que $\blacktriangleleft$ sea una relación de orden en B?
   1.b. Siendo por lo descubierto en el apartado 1.a., f tal que $\blacktriangleleft$ es una relación de orden en B, ¿es $(B; \boxplus, \boxtimes; \blacktriangleleft)$ un anillo ordenado?

[SEL 5:8] *Cfr.* Anzola y Caruncho [140]: problema 5.22 (pág. 107).

§ 17.18 Muestra de ejemplos finales

Ejemplo 513

Sea $\mathbb{B}$ el conjunto de todos los octetos. Sean $+$ y $\cdot$ la suma y el producto habitual en $\mathbb{Z}$. En $\mathbb{B}$ se consideran las operaciones $\boxplus$ y $\boxdot$, definidas, $\forall x_1x_2..x_8,\ y_1y_2..y_8 \in \mathbb{B}$, por $x_1x_2..x_8 \boxplus y_1y_2..y_8$ es el octeto cuyos bits son (x_1+y_1) mód 2, (x_2+y_2) mód 2, $\ldots$, (x_8+y_8) mód 2 (x mód y designa el resto de la división euclidea de x por y) (por ejemplo, $10110111 \boxplus 11011101 = 01101010$), y $x_1x_2..x_8 \boxdot y_1y_2..y_8$ es el octeto cuyos bits son $(x_1 \cdot y_1)$ mód 2, $(x_2 \cdot y_2)$ mód 2, $\ldots$, $(x_8 \cdot y_8)$ mód 2 (por ejemplo, $10110111 \boxdot 11011101 = 10010101$).

Demostrando cada una de las propiedades que correspondan, averigüemos todo lo que podamos sobre la estructura algebraica de: 0, $(\mathbb{B}; \boxplus)$; 1, $(\mathbb{B}; \boxdot)$, y 2, $(\mathbb{B}; \boxplus, \boxdot)$.

[EFE 14.7.2020:1b (p.h.e.c.)].

Resolución.— Pudiésemos trabajar directamente con dicho conjunto

$$\mathbb{B} = \{00000000, 00000001, 00000010, \ldots, 11111111\}$$

—en base 10, es el conjunto $\{0, 1, 2, \ldots, 255\}$— y las operaciones $\boxplus$ y $\boxdot$, tal como vienen definidas en el enunciado pero en lo primero que caemos en la cuenta es que $\forall x, y \in \{0, 1\}$,

$$(x+y) \text{ mód } 2 \leftrightarrow x \vee y,$$
$$(x \cdot y) \text{ mód } 2 \leftrightarrow x \wedge y,$$

esto es, $\boxplus$ y $\boxdot$ son, respectivamente, las operaciones XOR bit a bit[33] y AND bit a bit[34]. De hecho, el enunciado da por hecho que $\boxplus$ y $\boxdot$ son operaciones en $\mathbb{B}$, como en efecto lo son, por serlo $\veebar$ y $\wedge$ en $\{0, 1\}$ y además conocemos, por haberlas estudiado, sus propiedades básicas[35]. Estas operaciones $\boxplus$ y $\boxdot$ —XOR bit a bit y AND bit a bit, respectivamente— definen, dados $\boldsymbol{u} = u_0u_1\ldots u_7$ y $\boldsymbol{v} = v_0v_1\ldots v_7$, los octetos $\boldsymbol{u} \boxplus \boldsymbol{v}$ y $\boldsymbol{u} \boxdot \boldsymbol{v}$, por

$$\begin{aligned} \boldsymbol{u} \boxplus \boldsymbol{v} &= (u_1 \veebar v_1)(u_2 \veebar v_2)\ldots(u_8 \veebar v_8), \\ \boldsymbol{u} \boxdot \boldsymbol{v} &= (u_1 \wedge v_1)(u_2 \wedge v_2)\ldots(u_8 \wedge v_8). \end{aligned} \tag{17.13}$$

0. Estudiemos la estructura algebraica de $(\mathbb{B}; \boxplus)$.

---

[33] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Operador_a_nivel_de_bits#XOR.
[34] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Operador_a_nivel_de_bits#AND.
[35] *Cfr. supra* ejemplo 17.21 (pág. 935 de esta edición).

I. ¿Satisface $\boxplus$ la propiedad conmutativa en $\mathbb{B}$?

$$\begin{aligned} \boldsymbol{u} \boxplus \boldsymbol{v} &= (u_0 \veebar v_0)(u_1 \veebar v_1) \dots (u_7 \veebar v_7) \\ &\overset{(0)}{=} (v_0 \veebar u_0)(v_1 \veebar u_1) \dots (v_7 \veebar u_7) \\ &= \boldsymbol{v} \boxplus \boldsymbol{u} \end{aligned}$$

(0) Por satisfacer $\veebar$ la propiedad conmutativa en $\{0, 1\}$ —*cfr. supra* ejemplo 17.21 (pág. 935 de esta edición)—.

II. ¿Satisface $\boxplus$ la propiedad asociativa en $\mathbb{B}$?

$$\begin{aligned} \boldsymbol{u} \boxplus (\boldsymbol{v} \boxplus \boldsymbol{w}) &= \boldsymbol{u} \boxplus (v_0 \veebar w_0)(v_1 \veebar w_1) \dots (v_7 \veebar w_7) \\ &= (u_0 \veebar (v_0 \veebar w_0))(u_1 \veebar (v_1 \veebar w_1)) \dots (u_7 \veebar (v_7 \veebar w_7)) \\ &\overset{(1)}{=} ((u_0 \veebar v_0) \veebar w_0)((u_1 \veebar v_1) \veebar w_1) \dots ((u_7 \veebar v_7) \veebar w_7) \\ &= (u_0 \veebar v_0)(u_1 \veebar v_1) \dots (u_7 \veebar v_7) \boxplus \boldsymbol{w} \\ &= (\boldsymbol{u} \boxplus \boldsymbol{v}) \boxplus \boldsymbol{w} \end{aligned}$$

(1) Por satisfacer $\veebar$ la propiedad asociativa en $\{0, 1\}$ —*cfr. supra* ejemplo 17.21 (pág. 935 de esta edición)—.

III. ¿Tiene $\boxplus$ elemento neutro en $\mathbb{B}$? Esto es, ¿existe $\boldsymbol{e} = e_0e_1 \dots e_7 \in \mathbb{B}$ tal que para todo $\boldsymbol{u} = u_0u_1 \dots u_7 \in \mathbb{B}$, $u_0u_1 \dots u_7 = e_0e_1 \dots e_7 \boxplus u_0u_1 \dots u_7 = u_0u_1 \dots u_7 \boxplus e_0e_1 \dots e_7$? Por ser $\boxplus$ conmutativa en $\mathbb{B}$, buscamos sólo por un lado:

$$\begin{aligned} u_0u_1 \dots u_7 &= e_0e_1 \dots e_7 \boxplus u_0u_1 \dots u_7 \\ &= (e_0 \veebar u_0)(e_1 \veebar u_1) \dots (e_7 \veebar u_7) \\ &\to u_i = e_i \veebar u_i \\ &\overset{(2)}{\to} e_i = 0. \end{aligned}$$

Por lo tanto, $\boldsymbol{0} = 00000000$ es el elemento neutro de $\boxplus$ en $\mathbb{B}$.

(2) Por ser 0 el elemento neutro de $\veebar$ en $\{0, 1\}$ —*cfr. supra* ejemplo 17.21 (pág. 935 de esta edición)—.

IV. ¿Existe el elemento simétrico por $\boxplus$ de cualquier elemento de $\mathbb{B}$? Esto es, ¿para todo $\boldsymbol{u} = u_0u_1 \dots u_7 \in \mathbb{B}$, existe $\boldsymbol{u'} = u'_0u'_1 \dots u'_7 \in \mathbb{B}$ tal que $e_0e_1 \dots e_7 = u'_0u'_1 \dots u'_7 \boxplus u_0u_1 \dots u_7 = u_0u_1 \dots u_7 \boxplus u'_0u'_1 \dots u'_7$? Por ser $\boxplus$ conmutativa en $\mathbb{B}$, buscamos sólo por un

lado:

$$\begin{aligned} e_0 e_1 \dots e_7 &= 00 \dots 0 \\ &= u'_0 u'_1 \dots u'_7 \boxplus u_0 u_1 \dots u_7 \\ &= (u'_0 \veebar u_0)(u'_1 \veebar u_1) \dots (u'_7 \veebar u_7) \\ &\to 0 = u'_i \veebar u_i \\ &\overset{(3)}{\to} u'_i = u_i. \end{aligned}$$

Por lo tanto, cada elemento de $\mathbb{B}$ es su propio simétrico por $\boxplus$.

(3) Por definición de $\veebar$.

Por todo ello, $(\mathbb{B}; \boxplus)$ es un grupo abeliano.

1. Estudiemos la estructura algebraica de $(\mathbb{B}; \boxdot)$ (*cfr.* actividad 17.26 [pág. 939 de esta edición]).
2. Estudiemos la estructura algebraica de $(\mathbb{B}; \boxplus, \boxdot)$ (*cfr.* actividad 17.27 [pág. 939 de esta edición]).

■

Actividad 17.26

Con un estudio similar al hecho para $(\mathbb{B}; \boxplus)$ demostremos que $(\mathbb{B}; \boxdot)$ es un monoide abeliano, siendo 11111111 el elemento neutro.

Actividad 17.27

Con un estudio similar al hecho para $(\mathbb{B}; \boxplus)$ demostremos que $\boxdot$ es distributiva respecto de $\boxplus$, y por tanto que $(\mathbb{B}; \boxplus, \boxdot)$ es un anillo abeliano unitario.

Observación 17.18.0.— La estructura $(\mathbb{B}; \boxplus, \boxdot)$ no es dominio de integridad, ya que, por ejemplo, $01010101 \boxdot 10101010 = 00000000$; por lo tanto, tampoco es cuerpo.

Observación 17.18.1.— Alternativamente, pudiésemos estudiar esta cuestión en el ámbito de los conjuntos. Y esto es así porque $\veebar$ y $\wedge$ corresponden en el ámbito de los conjuntos a las operaciones diferencia simétrica $(\triangle)$ e intersección $(\cap)$, respectivamente. Siendo ahora un conjunto C cualquiera de 8 elementos, existe una aplicación biyectiva entre el conjunto $\mathbb{B}$ de octetos y el conjunto potencia 2^C —cada octeto es una codificación de un subconjunto de C de acuerdo a la pertenencia de los elementos de C al subconjunto; por ejemplo, si $C = \{a, b, c, d, e, f, g, h\}$, el subconjunto $\{b, d, g, h\}$ corresponde biyectivamente al octeto 01010011—. Todo consistiría, pues, en estudiar las estructuras algebraicas de $(2^C; \triangle)$, $(2^C; \cap)$ y $(2^C; \triangle, \cap)$, para un conjunto arbitrario C de 8 elementos.

§ 17.19 Bibliografía

- Estructuras.
  - Teoría.

[145] José García García y Manuel López Pellicer. *Álgebra lineal y geometría: curso teórico-práctico*. Marfil, Alcoy, Hoya de Alcoy, Alicante (ES-A), España, 8.ª ed., 1992.

[146] Armando Óscar Rojo. *Álgebra I*. El Ateneo, Buenos Aires (AR-C), Argentina, 1986. ©TDR.

[198] Alexei Ivanovich Kostrikin. *Introducción al álgebra*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1992. ©TDR.

  - Práctica.

[140] Máximo Anzola González y José Ramón Caruncho Castro. *Problemas de álgebra. Tomo 1: Conjuntos - Grupos*. Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1981. ©TDR.

[144] Agustín de la Villa Cuenca. *Problemas de Álgebra (con esquemas teóricos)*. CLAGSA, Madrid, Comunidad de Madrid (ES-M), España, 4.ª ed., 2010. ©TDR.

[197] Máximo Anzola González y José Ramón Caruncho Castro. *Problemas de álgebra. Tomo 2: Anillos - Polinomios - Ecuaciones.* Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1982. ©TDR.

[199] Alain Bigard, Maurice Crestey y Jacques Grappy. *Problemas de álgebra moderna*. Reverté, Barcelona, Cataluña (ES-CT), España, 1975. ©TDR.

- Específicamente acerca de Teoría de Grupos en SageMath y GAP.

  Desconozco si quien lee en este momento se dedica o dedicará profesionalmente o simplemente le atrae o atraerá algún campo de estudio que tenga relación con la teoría de grupos (como pudiese ser, por ejemplo, la codificación de la información[36]). De todos modos, estimo interesante que conozca que para la investigación básica en teoría de grupos, destaco GAP, si bien en una primera aproximación pudiésemos utilizar SageMath (que ya sabemos que admite los lenguajes Sage, Gap, GP, HTML, Macaulay2, Maxima, Octave, Python, R y Singular) —*cfr. supra* § 11 (pág. cii de esta edición)—.

  - Así, para SageMath, pudiese ser recomendable:

[36] *Cfr. v. gr.* Carlos Munuera Gómez y Juan Gabriel Tena Ayuso [200].

[201]Thomas William JUDSON y Robert Arnold BEEZER. *Abstract Algebra: Theory and Applications*. Autoedición, Nacogdoches, Condado de Nacogdoches, Texas (US-TX), Estados Unidos de América, 2022. http://abstract.ups.edu/sage-aata.html. ©GFDL.

(o bien https://doc.sagemath.org/html/en/thematic_tutorials/group_theory.html; de paso, ambas incluyendo indicaciones sobre cuestiones básicas de los números enteros, de nuestro interés para el estudio de la teoría de números).

- El lenguaje Gap que interpreta SageMath es propio de GAP (*Groups, Algorithms, Programming*)[37], un sistema algebraico computacional dedicado a la teoría de grupos; consultemos, por ejemplo:

[202]GAP SUPPORT GROUP. *GAP Documentation*, 2024. https://www.gap-system.org/Doc/-doc.html (accedido el 26.1.2024). ©gratis OA.

[203]Alexander HULPKE. *Using GAP*, 2000. https://www.math.colostate.edu/~hulpke/paper/gap4tut.pdf (accedido el 26.1.2024). ©gratis OA.

Si instalamos GAP podrían sernos de utilidad bibliotecas de terceras personas, por ejemplo, GroupExplorer[38] de Nathan CARTER.

- De hecho, en el apartado *Teaching*[39] de la documentación de GAP, encontramos dos materiales en español que se muestran muy interesantes para andar los primeros pasos en GAP:
  - Una introducción al álgebra con GAP, 2016, de Leandro VENDRAMIN, y
  - de Pedro A. García Sánchez[40]:
    - primeros pasos en GAP (https://www.ugr.es/~pedro/gap/primeros-pasos.pdf);
    - álgebra y estructuras discretas (https://www.ugr.es/~pedro/gap/practicas-GAP-AE.pdf);
    - matemáticas discretas (https://www.ugr.es/~pedro/gap/practicas-GAP-MD.pdf);
    - álgebra básica (https://www.ugr.es/~pedro/gap/practicas-GAP-AB.pdf);
    - bloque de GAP de la asignatura Software Matemáticas (https://github.com/pedritomelenas/Software-Matematicas-GAP/).

[37] *Cfr. v. gr.* https://www.gap-system.org/index.html y https://es.wikipedia.org/wiki/GAP_(sistema_algebraico_computacional).
[38] *Vid.* https://nathancarter.github.io/gap-pkg-groupexplorer/doc/chap0.html.
[39] *Vid.* https://www.gap-system.org/Doc/Teaching/teaching.html.
[40] Vid. https://algebra.ugr.es/pages/personal/fichas_profesores/pedro.

El juego de la vida (Conway). Autómatas celulares (von Neumann y Ulam). Un nuevo tipo de ciencia (Wolfram). El computador de Tinkertoy y otras maquinaciones (Dewdney)

Lógica, clases, relaciones, estructuras, todas ellas presentes en el *juego de la vida* (*vid. v. gr.* https://es.wikipedia.org/wiki/Juego_de_la_vida), 1970, de John Horton Conway, que es, quizás, el *autómata celular* más conocido —si bien los orígenes de estos últimos estén en John von Neumann y Stanislaw Ulam—. Nada más que nos informemos un poco, podremos comprobar que las aplicaciones de los autómatas celulares son variadas en múltiples campos (*vid. v. gr.* https://en.wikipedia.org/wiki/Cellular_automaton#Applications).

Si disponemos de tiempo y deseamos saber más de ellos* (como, por ejemplo, de la Regla 110†, que resulta ser un autómata celular Turing completo —esto es, equivalente a una máquina universal de Turing—‡, al igual que el juego de la vida de Conway), una buena opción es el libro *A New Kind of Science*, de Stephen Wolfram —el creador de Wolfram|Alpha y del lenguaje Mathematica—, cuya versión en línea es enteramente accesible (*vid.* https://www.wolframscience.com/nks/), libro, que bien está decirlo, como todo en este mundo, cuenta con sus partidarios y detractores (*cfr. v. gr.* https://es.wikipedia.org/wiki/Un_nuevo_tipo_de_ciencia, sin embargo, *A New Kind of Science* es un libro que puede proporcionarnos multitud de ideas en variados campos; si tenemos tiempo e inquietudes, echémosle un buen ojo.

Y, hablando de ideas, también cuando tengamos tiempo, es recomendable el libro *The Tinkertoy Computer and other machinations* (*vid. v. gr.* https://archive.org/details/tinkertoycomputer00dewd/mode/2up), de Alexander Keewatin Dewdney (Tinkertoy es un juego de construcción parecido a Lego). Echemos un vistazo al índice de este libro, casi seguro que nos sorprenderá —este ejemplar procede de la Bell Book Collection (*vid.* https://archive.org/details/thecomputermuseumarchive?tab=collection), en el Archivo de Internet (*vid.* https://es.wikipedia.org/wiki/Internet_Archive)—.

* Por cierto y por ejemplo, con este artefacto en línea, pudiésemos generarlos: https://kidojo.com/cellauto/generate.cgi.

† *Vid. v. gr.* https://en.wikipedia.org/wiki/Elementary_cellular_automaton.

‡ *Vid. v. gr.* https://en.wikipedia.org/wiki/Turing_completeness.

Parte II

Teoría de números elemental

Dedicamos esta parte a un estudio introductorio de la *teoría de números elemental*. En ella usaremos estrategias aritméticas, geometría, álgebra y cálculo de un nivel básico. Un estudio más profundo nos llevaría a la *teoría algebraica de números* y a la *teoría analítica de números*, en las que, llegado el caso, usaríamos estrategias de álgebra avanzada y de análisis matemático avanzado, respectivamente. No obstante, no se trata de una división nítida; en ciertos casos es necesario utilizar combinaciones de estrategias de diferentes campos.

CAPÍTULO 18

Teoría de números

> Cada día que amanece, el número de los tontos crece.
>
> (Refrán).

¿Por qué nos cuesta imaginar un universo donde los números primos sean otros? Porque, por ejemplo, sí que concebimos geometrías no euclideas.°

° Más alla de lugares como el del ejemplo 523 (pág. 960 de esta edición).

§ 18.0 Divisibilidad en el anillo de los enteros

En realidad, $(\mathbb{Z}; +, \cdot)$ es un dominio de integridad, ya que es un anillo abeliano, unitario e íntegro.

§ 18.0.0 Conceptos y primeras propiedades

Definición 18.0.— Dados $d, n \in \mathbb{Z}$, decimos que d *divide a* n (hecho que designamos por $d \mid n$) si, y sólo si, $\exists c \in \mathbb{Z}$, tal que $n = cd$. Sinónimamente, decimos que d es *divisor de* n, d es un *factor de* n, d es un *submúltiplo de* n, n es *divisible por* d o que n es *múltiplo de* d.

Si d *no divide* a n, lo notamos $d \nmid n$.

Observación 18.0.0.— d divide a n si, y sólo si, $|d|$ divide a $|n|$ (designando $|x|$ el valor absoluto de x).

Definición 18.1.— Los *divisores triviales* de n son $-1, 1, -n$ y n.

Definición 18.2.— Llamamos *parte alícuota* (o, sinónimamente, *divisor propio*), de n a todo divisor positivo de n distinto de n.

Notamos por $D(n)$ el *conjunto finito de los divisores positivos de* n, por $M(n)$ el *conjunto infinito de los multiplos positivos de* n y por $M_0(n)$ el *conjunto infinito de los multiplos no negativos de* n.

Teorema 18.0 (La relación de divisibilidad es un preorden parcial en $\mathbb{Z}$)
$\forall d, m, n \in \mathbb{Z}$:
0. $n \mid n$; (reflexiva)
1. $d \mid m \wedge m \mid n \to d \mid n$. (transitiva)

Por esto decimos que $(\mathbb{Z}, +, \cdot)$ es un dominio de integridad (unitario) preordenado parcialmente por $\mid$.

Teorema 18.1 (Otras propiedades)

$\forall d, n \in \mathbb{Z}$:

2. $-n \mid n$;
3. $d \mid n \leftrightarrow -d \mid n \leftrightarrow d \mid -n \leftrightarrow -d \mid -n$;
4. $-1 \mid n$ y $1 \mid n$; (−1 y 1 son divisores universales)
5. $d \mid 1$ si, y sólo si, $d = -1$ o $d = 1$; (1 sólo es múltiplo de −1 y de 1)
6. si $d \mid n$ y $n \mid d$, entonces $d = -n$ o $d = n$;
7. $d \mid 0$; (0 es múltiplo de todo entero)
8. si $0 \mid n$, entonces $n = 0$. (0 sólo divide a 0)

Teorema 18.2 (Propiedades algebraicas)

$\forall a, b, d, m, n \in \mathbb{Z}$:

9. si $d \mid m$ y $b \mid n$, entonces $db \mid mn$;
10. si $d \mid m$ y $d \mid n$, entonces:
    a. $d \mid (m + n)$; (aditiva)
    b. $d \mid am$; (producto por escalar entero)
    c. $d \mid bn$; (producto por escalar entero)
    d. $d \mid (am + bn)$. (linealidad entera)

Teorema 18.3 (Propiedades de multiplicación y simplificación)

$\forall a, d, n \in \mathbb{Z}$:

11. si $d \mid n$, entonces $ad \mid an$; (multiplicación)
12. si $ad \mid an$ y $a \neq 0$, entonces $d \mid n$. (cancelación/simplificación)

Teorema 18.4 (Propiedades de orden)

$\forall d, n \in \mathbb{Z}$:

13. si $d \mid n$ y $n \neq 0$, entonces $|d| \leq |n|$; (comparación)
14. si $d \mid n$ y $d, n \in \mathbb{Z}^+$, entonces $d \leq n$.

Teorema 18.5 (No antisimetría de $\mid$ en $\mathbb{Z}$)

$\forall d, n \in \mathbb{Z}$:

15. si $d \mid n$ y $n \mid d$, entonces $|d| = |n|$; ($\mid$ no es antisimétrica en $\mathbb{Z}$)

Dos números enteros d y n tales que $d \mid n$ y $n \mid d$ y $d \neq n$ se llaman *asociados*.

Observación 18.0.1.— En realidad, se define el concepto de *elementos asociados en un dominio de integridad*. Sea $(D; +, \cdot)$ un dominio de integridad; x e y son elementos asociados en D si, y sólo si, ambos son divisores el uno del otro, esto es, si, y sólo si, $x \mid y$ e $y \mid x$. Ser x e y asociados equivale a

que exista una unidad u de $\langle D, +, \cdot \rangle$ tal que $u \cdot x = y$ (y, por tanto, tal que $x = u^{-1} \cdot y$), y también a que $(x) = (y)$, donde (x) e (y) designan los ideales generados por x e y, respectivamente.

Teorema 18.6 (Antisimetría de de $|$ en $\mathbb{N}$ y en Z^+)
$\forall d, n \in \mathbb{Z}$:
16. si $d \,|\, n$, $n \,|\, d$ y $d, n \in \mathbb{N}$, entonces $d = n$. (antisimétrica en $\mathbb{N}$)
(que también se satisface si $d, n \in \mathbb{Z}^+$)

Por el teorema 18.0 (pág. 947 de esta edición) y el teorema 18.6 (pág. 949 de esta edición), $|$ es una relación de *orden parcial en* $\mathbb{N}$ y *en* $\mathbb{Z}^+$. Decimos que el semianillo abeliano y unitario $(\mathbb{Z}^+, +, \cdot)$ y el anilloide (*ringoid*) asociativo $(\mathbb{Z}^+, +, \cdot)$ están ordenados parcialmente por $|$.

Teorema 18.7 (Propiedad del divisor conjugado)
$\forall d, n \in \mathbb{Z}$, con $d \neq 0$:
17. si $d \,|\, n$, entonces $(n/d) \,|\, n$; (el número n/d se llama *divisor conjugado* de d —respecto de n—).

Actividad 18.0

Demostremos los teoremas anteriores.

Con miras a su resolución.— A modo de ejemplos: 1., la transitividad de $|$ en $\mathbb{Z}$, esto es, $\forall d, m, n \in \mathbb{Z}$, $d \,|\, m \wedge m \,|\, n \to d \,|\, n$, en efecto, de $d \,|\, m$, $\exists k \in \mathbb{Z}$ tal que $m = d \cdot k$, y de $m \,|\, n$, $\exists k' \in \mathbb{Z}$ tal que $n = m \cdot k'$, por lo tanto, $\exists k'' \in \mathbb{Z}$ $(k'' = k \cdot k')$ tal que $n = d \cdot k''$; 15., la no antisimetría de $|$ en $\mathbb{Z}$, en efecto, de $m \,|\, n \wedge n \,|\, m$, $\exists k, k' \in \mathbb{Z}$ tal que $n = k \cdot m$ y $m = k' \cdot n$, por lo que $n = k \cdot k' \cdot n$, de donde, $k \cdot k' = 1$, por lo que, $k = k' = 1$ o $k = k' = -1$, de donde, $m = n$ o $m = -n$, esto es, $|m| = |n|$.

§ 18.0.1 Algoritmo de la división (euclidea)

Teorema 18.8 (Algoritmo de la división (euclidea))
Dados $D, d \in \mathbb{Z}$, existen dos únicos enteros q y r tales que $D = dq + r$ y $0 \leq r < |d|$; D, d, q y r se denominan *dividendo*, *divisor*, *cociente* y *resto*, respectivamente.

Observación 18.0.2.— Exigimos que el resto sea no negativo; por ejemplo, si el dividendo es -7 y el divisor es 3, el cociente es -3 y el resto 2, esto es, $-7 = 3 \cdot (-3) + 2$, ésta es la división euclidea y no $-7 = 3 \cdot (-2) + (-1)$.

Si $D = dq + r$ y $0 \leq r < |d|$, notamos $D \operatorname{div} d = q$ y $D \operatorname{mód} d = r$.

Observación 18.0.3.— Con respecto al teorema 18.8 (pág. 949 de esta edición), se satisfacen, $\forall D \in \mathbb{Z}$ y $\forall d \in \mathbb{Z}^+$:

18. $d \mid D$ si, y sólo si, existe un único entero q tal que $D = dq$, en otras palabras, si, y sólo si, $r = 0$;
19. si $d = 0$, entonces $r = D$ pero q no es único;
20. dado un divisor d, sólo hay $|d|$ restos posibles, a saber, 0, 1, . . ., $|d| - 1$.

Teorema 18.9 (Sumas de pares e impares)

Se satisface:

21. la suma de un número par y un número impar es un número impar;
22. toda suma de números pares es par;
23. toda suma de un número par de números impares es par.

Teorema 18.10 (Potencias de pares e impares)

Se satisface:

24. toda potencia positiva de un número par es par;
25. toda potencia no negativa de un número impar es impar.

Demostración.—

24. Sean $m \in \mathbb{Z}$ y $n \in \mathbb{Z}^+$, entonces

$$\begin{aligned}(2m)^n &= 2^n \cdot m^n \\ &= 2 \cdot 2^{n-1} \cdot m^n,\end{aligned}$$

esto es, $\exists k \in \mathbb{Z}$ tal que $(2m)^n = 2k$, siendo k precisamente $2^{n-1} \cdot m^n$, que es entero por serlo m y n.

25. Sean $m \in \mathbb{Z}$ y $n \in \mathbb{N}$, entonces por inducción débil: $(2m+1)^0 = 1$, impar; si $(2m+1)^i$ es impar, entonces $(2m+1)^{i+1} = (2m+1)^i(2m+1) = 2m(2m+1)^i + (2m+1)^i$, esto es, la suma de un par y un impar, que es impar. ■

Teorema 18.11 (Suma impar de enteros consecutivos)

Se satisface:

26. si n es impar, la suma de n números enteros consecutivos es múltiplo de n.

Demostración.— Sea $m \in \mathbb{Z}$,

$$\begin{aligned}(m+1) + (m+2) + \cdots + (m+n) &= nm + (1 + 2 + \cdots + n) \\ &= nm + \frac{n(n+1)}{2}\end{aligned}$$

$$= n\left(m + \frac{n+1}{2}\right),$$

y como n es impar, $2\,|\,(n+1)$, por lo que $m + (n+1)/2$ es un número entero y, por lo tanto, la suma $(m+1) + (m+2) + \cdots + (m+n)$ es múltiplo de n. ■

Ejemplo 514

Demostremos que $\forall n \in \mathbb{Z}$, $n(n+1)(2n+1)/6 \in \mathbb{Z}$.

Sugerencia.— Sea $p = n(n+1)(2n+1)$; usemos el algoritmo de la división para $D = n$ y $d = 6$, para demostrar después que el resto de la división de p por 6 es cero.

[EFO 20.5.2022:5a].

Resolución.— Por el algoritmo de la división, existen dos únicos enteros q y r tales que $n = 6q + r$ y $0 \leq r < 6$. Entonces,

$$\begin{aligned} p &= n(n+1)(2n+1) = 2n^3 + 3n^2 + n \\ &= 2(6q+r)^3 + 3(6q+r)^2 + 6q + r \\ &= 432q^3 + 216q^2r + 36qr^2 + 2r^3 + 108q^2 + 36qr + 3r^2 + 6q + r \\ &= 6(72q^3 + 36q^2r + 6qr^2 + 18q^2 + 6qr + q) + 2r^3 + 3r^2 + r, \end{aligned}$$

luego $\exists k \in \mathbb{Z}$ tal que $p = 6k + 2r^3 + 3r^2 + r$, con $0 \leq r < 6$.

Para conseguir el objetivo nos interesa demostrar que para $0 \leq r < 6$, $6\,|\,(2r^3 + 3r^2 + r)$.

Aventurémonos en una demostración por casos; ¿conseguiremos demostrar que para todos los valores válidos de r, 6 divide a p?

Pues sí, en efecto,

$$\begin{aligned} &r = 0 \to p = 6k \to 6\,|\,p, \\ &r = 1 \to p = 6k + 2\cdot 1^3 + 3\cdot 1^2 + 1 = 6k + 6 = 6k + 6\cdot 1 = 6\cdot(k+1) \to 6\,|\,p, \\ &r = 2 \to p = 6k + 2\cdot 2^3 + 3\cdot 2^2 + 2 = 6k + 30 = 6k + 6\cdot 5 = 6\cdot(k+5) \to 6\,|\,p, \\ &r = 3 \to p = 6k + 2\cdot 3^3 + 3\cdot 3^2 + 3 = 6k + 84 = 6k + 6\cdot 14 = 6\cdot(k+14) \to 6\,|\,p, \\ &r = 4 \to p = 6k + 2\cdot 4^3 + 3\cdot 4^2 + 4 = 6k + 180 = 6k + 6\cdot 30 = 6\cdot(k+30) \to 6\,|\,p, \\ &r = 5 \to p = 6k + 2\cdot 5^3 + 3\cdot 5^2 + 5 = 6k + 330 = 6k + 6\cdot 55 = 6\cdot(k+55) \to 6\,|\,p. \end{aligned}$$ ■

Observación 18.0.4.— Una demostración por casos famosa fue la del teorema de los cuatro colores[1], en 1976, en la que Kenneth Ira APPEL y Wolfgang HAKEN redujeron la infinitud de mapas

---

[1] *Vid. v. gr.* https://en.wikipedia.org/wiki/Four_color_theorem.

posibles a 1834 configuraciones que tuvieron que ser comprobadas una a una por computador, lo que llevó unas mil horas de tiempo de cómputo.

Actividad 18.1

Demostremos que si n es un número entero, entonces $n(n+1)(n+2)/6$ también lo es. *Sugerencia.*— Pudiésemos intentar resolverla por el algoritmo de la división —de forma similar a como hemos resuelto el ejemplo anterior—, o quizás pudiésemos intentar una inducción sobre n, o, cuando sepamos más de razonamiento combinatorio, vía una demostración combinatoria[2].

Actividad 18.2

Demostremos que si n es entero, entonces n es par si, y sólo si, n^2 es par.

[Cubit 108].

Actividad 18.3

Aprendamos el teorema del resto (también conocido como *teorema pequeño de* BÉZOUT) (*vid. v. gr.* https://es.wikipedia.org/wiki/Teorema_del_resto); utilicémoslo para demostrar que si n es impar y $a \neq -b$, entonces $a+b$ divide a $a^n + b^n$ (siendo $a, b \in \mathbb{Z}$).

El teorema de PICK (1899)

A propósito de números enteros, el teorema de PICK[*] asegura que podemos calcular el área de un polígono reticular, esto es, de un polígono simple con vértices con coordenadas enteras, contando el número de puntos de su frontera que tienen coordenadas enteras (F) y el número de puntos en su interior que tienen coordenadas enteras (I):

$$A = I + \frac{F}{2} - 1.$$

[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/Pick's_theorem.

[2] Cuando estudiemos el capítulo Razonamiento Combinatorio nos daremos cuenta de que $n(n+1)(n+2)/6 = C(n+2,3)$ esto es, el número de combinaciones de tres elementos de un conjunto de $n+2$ elementos, siendo una posible interpretación el número de subconjuntos de tres elementos de dicho conjunto, siempre que $3 \leq n+2$. Caso contrario, si $n+2 < 3$, es decir, si $n < 1$, entonces: por un lado, si $n = 0$, $n = -1$ o $n = -2$, el número es cero que es entero; por otro, si $n \leq -3$, entonces $n(n+1)(n+2) < 0$, por lo que consideramos sus correspondientes positivos y $|n(n+1)(n+2)|/6 \in \mathbb{Z}$ (ya ha sido analizado antes, pues $3 \leq |n|$), así que, $n(n+1)(n+2)/6 = -|n(n+1)(n+2)|/6$.

§ 18.1 Sistemas de numeración

Un *sistema de numeración* es un sistema de escritura para representar números.[3] En este subcapítulo nos centramos en la *notación posicional de los números*, uno de los mayores descubrimientos en la matemática.

Definición 18.3.— Dado un número $b \in \mathbb{N}_{\geq 2}$ al que denominamos *base*, entonces todo número natural n puede escribirse de manera única como

$$n = n_0 + n_1 \cdot b + n_2 \cdot b^2 + \cdots + n_k \cdot b^k,$$

con $n_k \neq 0$ y $0 \leq n_i < b$, para todo $i \in \mathbb{N}_{<k+1}$. Dicha expresión única la llamamos *expresión polinómica del número n en base b*.

Definición 18.4.— La que llamamos *expresión de un número n en base b* está determinada por los coeficientes n_i de la expresión polinómica única de n en base b y la escribimos

$$(n_k n_{k-1} \ldots n_1 n_0)_b$$

o

$$n_k n_{k-1} \ldots n_1 n_{0(b}$$

por ejemplo, $(123)_4$ o $123_{(4}$.

Teorema 18.12
Para transformar la expresión de un número en base b a su expresión en base 10, basta hacer las operaciones implicadas en la expresión.

Ejemplo 515

Hallemos las expresiones decimales de los números $(201)_3$ y $(2F1)_{16}$.

Resolución.— Las expresiones polinómicas de estos números en base 10 son: $(201)_3 = 2 \cdot 3^2 + 0 \cdot 3^1 + 1 \cdot 3^0 = 19$ y $(2F1)_{16} = 2 \cdot 16^2 + 15 \cdot 16^1 + 1 \cdot 16^0 = 753$. ■

[3] *Vid. v. gr.* https://en.wikipedia.org/wiki/Numeral_system y https://en.wikipedia.org/wiki/List_of_numeral_systems.

Teorema 18.13
Para transformar la expresión de un número en base 10 a su expresión en base b, hemos de dividir sucesivamente por b todos los coeficientes n_i de la expresión polinómica en base b hasta que satisfagan que $0 \leq n_i \nless b$.

Ejemplo 516

Expresemos 1123 en el sistema de numeración duodecimal (base 12).

Resolución.— $1123 = 93 \cdot 12 + 7 = 93 \cdot 12^1 + 7 \cdot 12^0$, como $0 \leq 93 \nless b = 12$, dividimos 93 por 12, $93 = 7 \cdot 12^1 + 9 \cdot 12^0$, y sustituyendo, $1123 = 93 \cdot 12^1 + 7 \cdot 12^0 = (7 \cdot 12^1 + 9 \cdot 12^0) \cdot 12^1 + 7 \cdot 12^0 = 7 \cdot 12^2 + 9 \cdot 12^1 + 7 \cdot 12^0 = (797)_{12}$; en definitiva, el número decimal 1123 es $(797)_{12}$ en el sistema de numeración duodecimal[4]. ■

Ejemplo 517

Obtengamos por un procedimiento aritmético las cifras en base 10 de 1123.

Resolución.— Basta dividir sucesivamente por 10: $1123 = 112 \cdot 10 + 3$, luego la cifra de las unidades es 3; $112 = 11 \cdot 10 + 2$, luego la cifra de las decenas es 2; $11 = 1 \cdot 10 + 1$, luego la cifra de las centenas es 1; $1 = 0 \cdot 11 + 1$, luego la cifra de las unidades de millar es 1. ■

Ejemplo 518

Obtengamos por un procedimiento aritmético las cifras en base 12 de $(797)_{12}$.

Resolución.— Transformemos el número a base 10 y dividamos sucesivamente por 12. En efecto: por un lado, $(797)_{12} = 7 \cdot 12^2 + 9 \cdot 12^1 + 7 \cdot 12^0 = 1123$, por otro, $1123 = 93 \cdot 12 + 7$, luego la cifra de las unidades es 7; $93 = 7 \cdot 12 + 9$, luego la cifra de las docenas es 9; $7 = 0 \cdot 12 + 7$, luego la cifra de las gruesas[5] es 7. ■

[4] *Vid. v. gr.* https://es.wikipedia.org/wiki/Sistema_duodecimal.

[5] Una *gruesa* son doce docenas y una *gran gruesa*, doce gruesas (*vid. v. gr.* https://es.wikipedia.org/wiki/Gruesa); y ya que hablamos de docenas, no está de más conocer la *docena del panadero* (*vid. v. gr.* https://es.wikipedia.org/wiki/Docena_del_panadero).

Ejemplo 519

Sabemos que la suma de todos los números distintos de dos cifras que pueden formarse con tres cifras distintas a, b, c, es igual a 198; entonces:

0. ¿cuáles son a, b, c?
1. ¿y si a, b, c son consecutivas?

[Cubit 107].

Resolución.— Los números son:

- de dos cifras iguales, $10a + a$, $10b + b$ y $10c + c$;
- de dos cifras distintas, $10a + b$, $10b + a$, $10a + c$, $10c + a$, $10b + c$ y $10c + b$.

La suma de todos ellos es $33a + 33b + 33c$, por lo que la hipótesis es

$$33a + 33b + 33c = 198,$$

de aquí, $a + b + c = \dfrac{198}{33} = 6$, por tanto,

0. a, b, c tales que $a + b + c = 6$;
1. si son consecutivas, por ejemplo, $a = b - 1$, b, $c = b + 1$, entonces $a + b + c = (b - 1) + b + (b + 1) = 3b$, por lo que $3b = 6$ y, por tanto, $a = 1$, $b = 2$ y $c = 3$. ∎

Ejemplo 520

(Matemagia [adivinación y mentalismo]).— Le decimos a una persona: «Piense usted un número, no nos lo ponga muy difícil, por ejemplo, en base 10 y de 4 cifras. Reste del número la suma de sus cifras. Tache una cifra del resultado (no tache el cero —no nos lo ponga tan fácil—) y díganos la suma de las cifras restantes, que le diremos la cifra que ha tachado».

¿Por qué siempre es así, independientemente del número de cifras?

[Cubit 109].

Resolución.— $10^3a_3 + 10^2a_2 + 10a_1 + a_0 - (a_0 + a_1 + a_2 + a_3) = 9a_1 - 99a_2 - 999a_3$; esto es, al restar la suma de las cifras a un número el resultado es múltiplo de 9, por lo que imaginemos que el número original es 9999, entonces $9999 - 36 = 9963$ y si, por ejemplo, tachamos el 3, $9 + 9 + 6 = 24$, entonces el múltiplo de 9 mayor más próximo es 27 y $27 - 24 = 3$, esto es, se tachó el 3. Observemos

que pedimos que no tache un cero para poder decir 9 si el resultado que nos dicen es múltiplo de 9 —si pudiesen tachar un cero, entonces tendríamos que decir que podría ser cero o nueve—.[6] ■

Ejemplo 521

Dicen algunos textos que John Napier se pasó toda una noche sin dormir porque su sobrino le comentó que sabía las tablas de multiplicar hasta la del cinco y que era incapaz de aprenderse las siguientes, y que a la mañana siguiente le sugirió el siguiente método: utilizar los dedos de las manos, tras hacer la asignación de números: 6 $\leftrightharpoons$ pulgar, 7 $\leftrightharpoons$ índice, 8 $\leftrightharpoons$ medio, 9 $\leftrightharpoons$ anular y 10 $\leftrightharpoons$ meñique; de manera que si, por ejemplo, quieres multiplicar 6 por 8 juntes el pulgar de una mano con el medio de la otra, cuentes cuántos dedos quedan desde la unión hacia arriba, 4 en este caso, que serán las decenas y multipliques los que quedan por debajo, los de una mano por los de la otra, 4 por 2 es 8, que serán las unidades (si las unidades superan la decena, ésta sumaría como tal: por ejemplo, para calcular 6 por 6, juntamos ambos pulgares, quedando dos dedos arriba —dos decenas— y cuatro dedos abajo en cada mano, esto es, 4 por 4, o sea, 16, es decir, una decena y 6 unidades, en definitiva, 3 decenas y 6 unidades, por lo que el resultado es 36).

Resolución.— Reescribamos la asignación: $5+1 \leftrightharpoons$ pulgar, $5+2 \leftrightharpoons$ índice, $5+3 \leftrightharpoons$ medio, $5+4 \leftrightharpoons$ anular y $5+5 \leftrightharpoons$ meñique; notemos por $5+a$ los dedos de la mano derecha y $5+b$ los de la izquierda; según el método de Napier, las decenas son $10(a+b)$, resultado al que se le suma el producto $(5-a)\cdot(5-b)$ (n.º de dedos de la mano derecha por debajo × n.º de dedos de la mano izquierda por debajo); en definitiva: $10(a+b)+(5-a)\cdot(5-b)$, que expandido queda $25+5a+5b+ab$, lo que coincide con el producto de dos números $x, y \in [6,10]$: $x\cdot y=(5+a)\cdot(5+b)=25+5a+5b+ab$. ■

Actividad 18.4

Disponemos de un juego de diez pesas con las primeras potencias de tres: 1 cg, 3 cg, 9 cg, 27 cg, 81 cg, . . . , 19 683 cg. Con una balanza de precisión, ¿cómo comprobaríamos que un cuerpo pesa 7879 cg?

Con miras a su resolución.— Como $7879 = 3^0+3^1-3^2+3^3+3^4-3^5-3^6+3^7+3^8$, bastaría con colocar en un platillo el cuerpo y las pesas con signo negativo (3^2, 3^5 y 3^6), y en el otro, las pesas con signo positivo (3^0, 3^1, 3^3, 3^4, 3^7 y 3^8).

[6] Sobre matemagia, *vid. etiam infra* las actividades 18.26, 18.59, 18.61, 18.62 y 18.63 (págs. 1031, 1106, 1106, 1106 y 1107, respectivamente) y en el cuadro de la página 1190.

§ 18.2 Primos y el teorema fundamental de la aritmética

§ 18.2.0 Número primo

Definición 18.5.— Decimos que $n \in \mathbb{N}_{\geq 2}$ es un *número primo* si, y sólo si, tiene, y sólo tiene, como únicos divisores positivos sus divisores triviales positivos, 1 y n, esto es, precisamente si su única parte alícuota es 1. Utilizamos $\mathbb{P}$ para designar el conjunto de números primos.

Teorema 18.14
Un número $n \in \mathbb{N}_{\geq 2}$ es primo precisamente si es *no factorizable*, esto es, si, y sólo si, no puede escribirse como producto $p = ab$ con $2 \leq a < p$ y $2 \leq b < p$.

Definición 18.6.— Decimos que $n \in \mathbb{N}_{\geq 2}$ es un *número compuesto* si, y sólo si, no es un número primo.

Teorema 18.15
Todo número $n \in \mathbb{N}_{\geq 2}$ es primo o producto de números primos.

Teorema 18.16 (de Euclides)
Existen infinitos números primos, esto es, el conjunto de los números primos es infinito, en otras palabras, no existe un primo mayor que los demás.

Demostración.— (de Euclides, c. 300 a.C., *Elementos*, Libro IX)
Por reducción al absurdo. Supongamos que sí existe un primo mayor que los demás, un último primo, sea p_n tal último primo, escribamos todos los números primos en orden creciente $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, etc., siendo p_k el kaésimo primo, entonces el conjunto finito de todos los primos sería $\{p_i : 1 \leq i < n+1\}$ (p_n sería el último primo, el mayor primo). Sea

$$z = \prod_{i=1}^{n} p_i + 1,$$

entonces pueden suceder sólo dos cosas, o z es primo o no lo es; si z es primo, contradicción, ya que habíamos supuesto que el mayor era p_n si z no es primo, entonces algún primo p divide a z [por definición de número primo], pero p no puede ser ninguno de los p_i ($1 \leq i < n+1$), porque al dividir z por cualquiera de ellos el resto siempre es 1 y no 0, así que p es otro primo, pero eso es imposible porque hemos supuesto que p_n es el mayor primo. ■

Observación 18.2.0.— En mi opinión, una de las demostraciones más elegantes de la matemática es ésta, justo la que acabamos de estudiar, la de Euclides de la infinitud de los números primos.

La he contado tal como me la enseñaron, sin embargo, puede que las cosas no sucediesen así (pudiésemos leer, por ejemplo, *Prime Simplicity*, de Michael HARDY y Catherine WOODGOLD[7]).

Observación 18.2.1.— En el libro *Proofs from The Book*[8], de Martin AIGNER y Günter M. ZIEGLER, encontramos seis demostraciones diferentes del teorema de Euclides (la 6.ª edición del libro[9] incluye, en realidad, un número «infinito» de demostraciones).

Observación 18.2.2.— Aunque nos ha quedado claro que no existe un último primo, no cesan de buscarse primos grandes, nuevos miembros de la sucesión de primos[10].

Actividad 18.5

Demostremos que para todo entero positivo n existen n números compuestos consecutivos.[*]

[Cubit 110].

[*] Una vez resuelta esta actividad, no antes, este artículo pudiese ser un buen comienzo para quienes nos interese profundizar en el tema de las lagunas sin primos: https://en.wikipedia.org/wiki/Prime_gap.

Observación 18.2.3.— A la vez que existen lagunas sin primos tan grandes como queramos (actividad anterior), existen parejas de primos que se diferencian en dos unidades (las conocidas como parejas de *primos gemelos*, desconociéndose si el número de éstas es infinito), por lo que aparentemente la distribución de los números primos en $\mathbb{N}$ es irregular. Sin embargo, sí se conoce la densidad de los primos en $\mathbb{N}$; si $\pi(x)$ designa el número de primos no superiores al número real x, se satisface que $\lim_{x\to\infty} \pi(x)\ln x/x = 1$, esto es, que $\pi(x) \approx x/\ln x$ (resultado conjeturado por GAUSS y demostrado por HADAMARD y DE LA VALLÉE-POUSSIN).

Observación 18.2.4.— No sólo lo comentado en la observación anterior; pensemos en la compatibilidad de la existencia de lagunas de tamaño arbitrario sin primos con:

- por un lado, el siguiente conjunto de conjeturas relacionadas entre sí:
  - la *conjetura de* ANDRICA[11]: $(\forall n \in \mathbb{Z}^+)\left(p_{n+1} - p_n < 2\sqrt{p_n} + 1\right)$, que acota superiormente la enésima diferencia de primos consecutivos;

[7] *Vid.* https://www.researchgate.net/profile/Michael-Hardy-13/publication/226338654_Prime_Simplicity/links/5fb18441299bf10c36831c1f/Prime-Simplicity.pdf.
[8] *Vid. v. gr.* https://en.wikipedia.org/wiki/Proofs_from_THE_BOOK y https://de.wikipedia.org/wiki/Satz_des_Euklid (artículo más completo, en alemán).
[9] *Vid.* https://link.springer.com/book/10.1007/978-3-662-57265-8.
[10] *Vid. v. gr.* http://primes.utm.edu/largest.html.
[11] *Vid. v. gr.* https://es.wikipedia.org/wiki/Conjetura_de_Andrica, https://www.gaussianos.com/la-conjetura-de-andrica-o-que-distancia-hay-entre-dos-numeros-primos-consecutivos/ y https://oeis.org/search?q=Andrica&go=Search.

- la *conjetura de* LEGENDRE[12] : $(\forall n \in \mathbb{Z}^+)$ $(\exists p, \text{primo})$ $(n^2 < p < (n+1)^2)$;
- la *conjetura de* BROCARD[13] : entre los cuadrados de dos primos consecutivos existen al menos cuatro primos;
- la *conjetura de* OPPERMANN[14] : $(\forall n \in \mathbb{Z}^+ \setminus \{1\})$ $(\exists p, q, \text{primos})$ $(n^2 - n < p < n^2 < q < n^2 + n)$;

- por otro, la existencia de progresiones aritméticas de números primos arbitrariamente largas (**teorema de GREEN-TAO**[15]).

§ 18.2.1 El teorema fundamental de la aritmética

Teorema 18.17 (Teorema fundamental de la aritmética)
Todo número $n \in \mathbb{N}_{\geq 2}$ puede descomponerse de manera única salvo el orden de los factores en producto de potencias de números primos,

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

con p_i primo, $1 \leq \alpha_i$ y $p_i \neq p_j$ si $i \neq j$ $(1 \leq i < k+1)$ $(1 \leq j < k+1)$. Esta descomposición de n se conoce como su *descomposición en factores primos* (o, sinónimamente, su *factorización canónica*). Los factores $p_i^{\alpha_i}$ se llaman *factores primarios*. La descomposición suele ordenarse en orden creciente de las bases, esto es, $p_i < p_j$ si $i \leq j$ $(1 \leq i < k+1)$ $(1 \leq j < k+1)$.

Demostración.— *Vid. supra* el ejemplo 416 (pág. 811 de esta edición) para la demostración de la existencia y la actividad 16.0 (pág. 811 de esta edición) para la demostración de la unicidad. ■

Observación 18.2.5.— En realidad, el teorema fundamental de la aritmética es válido para todo entero no nulo, salvo el orden y el signo.

Teorema 18.18
Se satisface:

0. $d \mid n$ si, y sólo si, la descomposición en factores primos de d divide a la descomposición en factores primos de n, esto es, en ésta figuran todos los factores primos de aquélla, si bien con exponentes mayores o iguales.
1. El divisor más pequeño de un número entero, en valor absoluto, es un número primo.

[12] *Vid. v. gr.* https://en.wikipedia.org/wiki/Legendre's_conjecture, https://oeis.org/A014085 y https://oeis.org/A007491.
[13] *Vid. v. gr.* https://en.wikipedia.org/wiki/Brocard's_conjecture y https://oeis.org/A050216.
[14] *Vid. v. gr.* https://en.wikipedia.org/wiki/Oppermann's_conjecture.
[15] *Vid. v. gr.* https://en.wikipedia.org/wiki/Green-Tao_theorem.

Ejemplo 522

¿Es todo producto de tres números pares positivos un múltiplo de 48?

[EFO 4.6.2021:5a].

Resolución.— No. Sirva de contraejemplo el siguiente. Como la descomposición única en factores primos de 48 (teorema fundamental de la aritmética) es $48 = 2^4 \cdot 3$, cualquier número natural de la forma 2^n con $n \geq 3$ es un producto de tres números naturales pares que no es múltiplo de 48 por no serlo de 3 al no incluir 3 como factor. ■

Ejemplo 523

Demostremos que el teorema fundamental de la aritmética no es válido en el conjunto $6\mathbb{N} + 1 = \{6k + 1 : k \in \mathbb{N}\} = \{1, 7, 13, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, \ldots\}$.

[Cubit 127].

Resolución.— En efecto, en este conjunto, son números primos 25, 55 y 121 —ya que sus únicos divisores en $6\mathbb{N} + 1$ son 1 y ellos mismos—, y 3025 admite dos descomposiciones en factores primos: $3025 = 25 \cdot 121$ y $3025 = 55^2$. ■

Observación 18.2.6.— Pudiésemos utilizar el artefacto en línea SageMath[16] y el siguiente programita en lenguaje Sage para hallar los números en un rango con más de una descomposición —es a modo de ejemplo, variemos el conjunto y el rango según queramos—:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
# generando los primeros 1000 elementos mayores que 1 de {6k+1 : k natural}
numeros = [6*k + 1 for k in range(1, 1001)]

# identificando los números primos en {6k+1 : k natural}
def es_primo_en_conjunto(num, conjunto):
        # un número de {6k+1 : k natural}\{1} es primo si, y sólo si, es su único divisor
        for n in conjunto:
                if n != num and num % n == 0:
                        return False
        return True
```

[16] *Cfr. supra* § 11 (pág. cii de esta edición).

```
# identificando los primos en {6k+1 : k natural}
primos_en_conjunto = [num for num in numeros if es_primo_en_conjunto(num, numeros)]

# mostrando los primeros 100 números del conjunto, en líneas de un máximo de 20
print('Primeros 100 números del conjunto:\n')
primeros_100 = numeros[:100]
for i in range(0, 100, 20):
        print(' '.join(str(x) for x in primeros_100[i:i+20]))
print()

# mostrando los primos entre los primeros 100 números del conjunto
primos_en_los_100 = [x for x in primeros_100 if x in primos_en_conjunto]
print('Primos entre los primeros 100 números del conjunto:\n')
for i in range(0, len(primos_en_los_100), 20):
        print(' '.join(str(x) for x in primos_en_los_100[i:i+20]))

# definiendo la función para encontrar todos los números
#con más de una factorización en factores primos distintos
def encontrar_numeros_con_multiples_factorizaciones(primos, conjunto):
        resultados = []
        for num in conjunto:
                factorizaciones = []
                for i in range(len(primos)):
                        for j in range(i, len(primos)):
                        if primos[i] * primos[j] == num:
                                factorizaciones.append((primos[i], primos[j]))
                if len(factorizaciones) > 1:
                        resultados.append((num, factorizaciones))
        return resultados

# encontrando todos los números con más de una factorización en factores primos distintos
resultados = encontrar_numeros_con_multiples_factorizaciones(primos_en_conjunto, numeros)

# mostrando el total de números encontrados en el rango
print()
print(f'Encontrados {len(resultados)} números con más de una factorización entre los primeros {
    ↪ len(numeros)} del conjunto;')
print('éstos son y éstas sus factorizaciones:\n')

# mostrando el resultado
for numero, factorizaciones in resultados:
        print(f'El número {numero} tiene las siguientes factorizaciones en factores primos:\n')
        for factorizacion in factorizaciones:
                print(f'{numero} = {factorizacion[0]} * {factorizacion[1]}')
        print()
```


Su ejecución proporciona:

```
Primeros 100 números del conjunto:

7 13 19 25 31 37 43 49 55 61 67 73 79 85 91 97 103 109 115 121
127 133 139 145 151 157 163 169 175 181 187 193 199 205 211 217 223 229 235 241
247 253 259 265 271 277 283 289 295 301 307 313 319 325 331 337 343 349 355 361
367 373 379 385 391 397 403 409 415 421 427 433 439 445 451 457 463 469 475 481
487 493 499 505 511 517 523 529 535 541 547 553 559 565 571 577 583 589 595 601

Primos entre los primeros 100 números del conjunto:

7 13 19 25 31 37 43 55 61 67 73 79 85 97 103 109 115 121 127 139
145 151 157 163 181 187 193 199 205 211 223 229 235 241 253 265 271 277 283 289
295 307 313 319 331 337 349 355 367 373 379 391 397 409 415 421 433 439 445 451
457 463 487 493 499 505 517 523 529 535 541 547 565 571 577 583 601

Encontrados 2 números con más de una factorización entre los primeros 1000 del conjunto;
éstos son y éstas sus factorizaciones:

El número 3025 tiene las siguientes factorizaciones en factores primos:

3025 = 25 * 121
3025 = 55 * 55

El número 4675 tiene las siguientes factorizaciones en factores primos:

4675 = 25 * 187
4675 = 55 * 85
```

§ 18.2.2 Divisor positivo

Definición 18.7.— Escribiendo todos los números primos en orden creciente $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, etc., siendo p_n el enésimo primo, cualquier entero positivo n, incluido el 1 puede expresarse como $n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$ con $\alpha_i \geq 0$. La llamamos *descomposición infinita de n en factores primos*.

Ejemplo 524

Hallemos las descomposiciones infinitas de 28 y 360 en factores primos.

Resolución.— Las descomposiciones infinitas de 28 y 360 en factores primos son:

- $28 = 2^2 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot \ldots;$
- $360 = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot \ldots$ ■

Teorema 18.19 (Forma de un divisor positivo)
Dado $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, con p_i primo y $\alpha_i \geq 1$ para $i = 1, 2, \ldots, k$, entonces todo divisor positivo d de n es de la forma $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$, con $0 \leq \beta_i \leq \alpha_i$ $(i = 1, 2, \ldots, k)$, en otras palabras, d es un sumando último del producto $(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdot \ldots \cdot (1 + p_k + p_k^2 + \cdots + p_k^{\alpha_k})$ (es decir, una vez expandido dicho producto, un número es divisor positivo de n si, y sólo si, es un sumando).

Teorema 18.20 (Número de divisores positivos)
Dado $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, con p_i primo y $\alpha_i \geq 1$ para $i = 1, 2, \ldots, k$, entonces el *número de divisores positivos* de n es el número de sumandos del producto anterior una vez expandido: $|D(n)| = (1+\alpha_1)\cdot(1+\alpha_2)\cdot\ldots\cdot(1+\alpha_k)$ [detrás de su porqué está el principio de la multiplicación (*vid. infra* § 19.1.1 —pág. 1138—)]; usando las *funciones divisor* —*vid. infra* § 18.4 (pág. 981)— es $\sigma_0(n)$, que suele designarse también por $d(n)$, $\upsilon(n)$ o $\tau(n)$.

Teorema 18.21 (Suma de los divisores positivos)
Dado $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, con p_i primo y $\alpha_i \geq 1$ para $i = 1, 2, \ldots, k$, entonces la *s* de n es el resultado del producto anterior en el que observemos que cada factor es la suma de los primeros términos de una progresión geométrica, $\dfrac{a_n \cdot r - a_1}{r - 1}$ y, por tanto, la suma es $\dfrac{p_i^{\alpha_i+1} - 1}{p_i - 1} \cdot \dfrac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \dfrac{p_k^{\alpha_k+1} - 1}{p_k - 1}$; usando las *funciones divisor* —*vid. infra* § 18.4 (pág. 981)— es $\sigma_1(n)$, que suele designarse también simplemente por $\sigma(n)$.

Teorema 18.22 (Suma de las partes alícuotas)
Dado $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, con p_i primo y $\alpha_i \geq 1$ para $i = 1, 2, \ldots, k$, entonces la *suma de las partes alícuotas* de n es $\sigma(n) - n$; usando las *funciones divisor* —*vid. infra* § 18.4 (pág. 981)— es $s(n)$, que suele designarse también por $\sigma'(n)$.

Ejemplo 525

Del número decimal 360, hallemos:

0. todos sus divisores positivos;
1. su número N de divisores positivos, esto es, $|D(360)|$;
2. la suma S de todos sus divisores positivos;
3. sus divisores que son cuadrados perfectos.

Resolución.— Procedamos.

0. $360 = 2^3 \cdot 3^2 \cdot 5$, esto es, $k = 3$, $(p_1, p_2, p_3) = (2, 3, 5)$ y $(a_1, a_2, a_3) = (3, 2, 1)$ en

$$(1 + p_1 + p_1^2 + \cdots + p_1^{a_1}) \cdot (1 + p_2 + p_2^2 + \cdots + p_2^{a_2}) \cdot \ldots \cdot (1 + p_k + p_k^2 + \cdots + p_k^{a_k});$$

así, cualquier divisor positivo de 360 es un sumando último (un término de la suma una vez expandido el producto) de

$$(1 + 2 + 2^2 + 2^3) \cdot (1 + 3 + 3^2) \cdot (1 + 5),$$

esto es,

$$\begin{aligned}(1 + 2 + 2^2 + 2^3) \cdot (1 + 3 + 3^2) \cdot (1 + 5) &= (1 + 2 + 2^2 + 2^3) \cdot (1 + 3 + 3^2 + 5 + 15 + 45)\\ &= 1 + 2 + 4 + 8 + 3 + 6 + 12 + 24 + 9 + 18 + 36\\ &+ 72 + 5 + 10 + 20 + 40 + 15 + 30 + 60 + 120\\ &+ 45 + 90 + 180 + 360;\end{aligned}$$

así,

$$D(360) = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360\};$$

1. $N = (1 + 3) \cdot (1 + 2) \cdot (1 + 1) = 24;$

2. la suma S de todos sus divisores positivos de 360 es

$$\begin{aligned}S &= \frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1}\\ &= \frac{15}{1} \cdot \frac{26}{2} \cdot \frac{24}{4}\\ &= 1170;\end{aligned}$$

3. como $360 = 2^3 \cdot 3^2 \cdot 5$, sus divisores cuadrados perfectos tienen que ser de la forma $2^{2a} \cdot 3^{2b}$, esto es, son los sumandos últimos de $(1 + 2^2) \cdot (1 + 3^2) = 1 + 3^2 + 2^2 + 2^2 3^2$; por tanto, los divisores cuadrados perfectos de 360 son 1, 9, 4 y 36. ■

Observación 18.2.7.— De manera similar a como hicimos en la observación 11.27.0 (pág. 660 de esta edición), pudiésemos utilizar el artefacto en línea SageMath[17] y el siguiente programita en lenguaje Sage para dibujar el diagrama de HASSE de $(D_{360}; |)$:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
D360 = Poset((divisors(360), attrcall("divides")), linear_extension=True)
D360.show()
```

[17] *Cfr. supra* § 11 (pág. cii de esta edición).

que devuelve la imagen que vemos en la figura 18.0 (pág. 965 de esta edición).

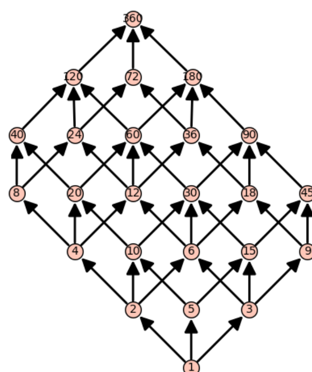


Figura 18.0.— Diagrama de Hasse de $(D_{360}; \,|\,)$. Resultado de la ejecución del programa anterior en SageMathCell. Observemos la particularidad de la representación por defecto con arcos (aristas dirigidas).

Ejemplo 526

¿Cuáles son los divisores cuadrados perfectos de 15 000?

Resolución.— Factorizando, resulta que $15\,000 = 2^3 \cdot 3 \cdot 5^4$; por lo tanto, los divisores cuadrados perfectos tienen que ser de la forma $2^{2a} \cdot 5^{2b}$, esto es, son los sumandos últimos de $(1+2^2)\cdot(1+5^2+5^4)$ y como $(1+2^2)\cdot(1+5^2+5^4) = 1+5^2+5^4+2^2+2^2 5^2+2^2 5^4$, los divisores cuadrados perfectos de 15 000 son 1, 25, 625, 4, 100 y 2500. ■

Observación 18.2.8.— Si quisiésemos conocer más sobre los cuadrados perfectos, ¿por qué no empezar por la propia sucesión 0, 1, 4, 9, 16, 25, . . ., catalogada como la sucesión A000290 en la OEIS[18]? La *OEIS (Enciclopedia en línea de las sucesiones de números enteros)* —fundada por Neil James Alexander Sloane[19]— es una fuente fundamental de conocimiento sobre sucesiones de números enteros, un gran catálogo donde se centraliza gran parte de la investigación sobre la mayoría de las más interesantes. En la Wikipedia en inglés encontramos la lista de todas las sucesiones de enteros catalogadas en la OEIS que tienen su propio artículo en la Wikipedia en inglés[20].

Por otra parte, el artefacto subyacente a la página web *Numbers Aplenty*, de Giovanni Resta, es capaz, cuando se consulta un número concreto, de analizar números bien grandes y sus propiedades, si bien hasta cierto límite[21], ofreciendo además páginas dedicadas a cada una de las propiedades destacadas. Por ejemplo, de éstas, la correspondiente a los cuadrados perfectos, https://www.numbersaplenty.com/set/square_number/, y en el caso de, digamos, el número 153, https://www.numbersaplenty.com/153.

[18] *Vid.* https://oeis.org/A000290.
[19] *Vid. v. gr.* https://oeis.org/wiki/User:N._J._A._Sloane.
[20] *Vid.* https://en.wikipedia.org/wiki/List_of_OEIS_sequences.
[21] *Vid.* https://www.numbersaplenty.com/limits.php.

Claro que los cuadrados perfectos son un caso particular de potencias perfectas, 1, 4, 8, 9, 16, 25, 27, 32, 36, . . ., catalogada como la sucesión A001597 en la OEIS[22] (*vid. etiam v. gr.* https://www.numbersaplenty.com/set/perfect_power/).

Echémosles un vistazo, a OEIS[23] y a Numbers Aplenty[24], pudiesen ser de nuestro interés.

Actividad 18.6

Hallemos $n \in \mathbb{Z}^+$ tal que $n = 2^a \cdot 5^b \cdot 7^c$, sabiendo que $5n$ tiene 8 divisores más que n y que $8n$ tiene 10 divisores más que $5n$.

[SEL 6:1].

¿Una representación numérica alternativa?

Algo que investigar, pero sólo si tenemos tiempo e inquietud. ¿Sería razonable representar 28 por 2001 y, en general, cualquier $n \in \mathbb{N}_{\geq 2}$, por $\alpha_1\alpha_2 \dots \alpha_k$, esto es, por los exponentes de los factores primos de la descomposición infinita de n, siendo α_k el último exponente no nulo? Por ejemplo,

$2 \mapsto 1,$	$6 \mapsto 11,$	$10 \mapsto 101,$
$3 \mapsto 01,$	$7 \mapsto 0001,$	$11 \mapsto 00001,$
$4 \mapsto 2,$	$8 \mapsto 3,$	$12 \mapsto 23,$
$5 \mapsto 001,$	$9 \mapsto 03,$	

y así sucesivamente.

Teorema 18.23

Todo número compuesto n tiene un divisor primo $p \leq \sqrt{n}$ o, lo que es equivalente, todo número n para el que no exista ningún primo $p \leq \sqrt{n}$ es un número primo.

Teorema 18.24 (Teorema $4n + 1$ de FERMAT)

(Conjeturado por FERMAT y demostrado por EULER).

Todo número primo de la forma $4n + 1$ es la suma de dos cuadrados.

Teorema 18.25 (Teorema de DIRICHLET, 1837)

Si a y b no tienen divisores comunes, entonces existen infinitos números primos de la forma $a \cdot n + b$.

---

[22] *Vid.* https://oeis.org/A001597.
[23] *Vid.* https://oeis.org/.
[24] *Vid.* https://www.numbersaplenty.com/.

Observación 18.2.9.— Para $n \in \mathbb{N}$, en recorrido creciente, los números $a \cdot n + b$ son b, $b + a$, $b + 2a$, $b + 3a$, . . ., esto es, una *progresión aritmética* entera de diferencia a y primer término b; por eso, también es conocido como teorema de DIRICHLET sobre progresiones aritméticas[25].

Teorema 18.26 (Postulado de BERTRAND, 1845; Teorema de (BERTRAND-)CHEBYCHEV, 1852)
$(\forall n \in \mathbb{N}_{>3})(\exists p \in \mathbb{P})(n < p < 2n - 2)$.

Observación 18.2.10.— Este teorema fue conjeturado por BERTRAND en 1845 y demostrado por CHEBYCHEV en 1852. Una formulación menos restrictiva es: $(\forall n \in \mathbb{N}_{>1})(\exists p \in \mathbb{P})(n < p < 2n)$.

Sin duda, el postulado de BERTRAND hace que pensemos de nuevo en la existencia, ya demostrada, de lagunas sin primos de tamaño arbitrario[26] y en la distribución de los números primos[27].

§ 18.3 Máximo común divisor y mínimo común múltiplo

§ 18.3.0 Máximo común divisor (mcd)

Definición 18.8.— Llamamos *divisor común* de a y b a cualquier número que divida a a y a b.

Lema 18.0.— Dados a y b, existe un divisor común d de a y b de la forma $d = sa + tb$, con s y t números, sucediendo además que todo divisor común de a y b divide a d.

Observación 18.3.0.— En breve, conoceremos éste como el *lema de* BÉZOUT y s y t como los *coeficientes de* BÉZOUT.

Teorema 18.27 (de existencia y unicidad del máximo común divisor)
Dados dos números a y b, existe un número d, y sólo uno, que satisface:
0.ª, $0 \leq d$ (d es no negativo);
1.ª, $d \mid a$ y $d \mid b$ (d es un divisor común de a y de b), y
2.ª, si $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$ (todo divisor común de a y de b divide a d).
El único d en estas condiciones se denomina *máximo común divisor* de a y b y se designa por $\mathrm{mcd}(a, b)$, aDb o simplemente (a, b).

Observación 18.3.1.— $\mathrm{mcd}(a, b) = 0$ si, y sólo si, $a = 0$ y $b = 0$; en cualquier otro caso, $\mathrm{mcd}(a, b) \geq 1$.

[25] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Teorema_de_Dirichlet_sobre_progresiones_aritméticas.
[26] *Vid. supra* actividad 18.5 (pág. 958 de esta edición).
[27] *Vid. supra* observación 18.2.3 (pág. 958 de esta edición).

Observación 18.3.2.— $\mathrm{mcd}(a, b)$ es precisamente el divisor común que satisface el lema 18.0 (pág. 967 de esta edición).

Observación 18.3.3.— Si d satisface el lema 18.0 (pág. 967 de esta edición), también lo satisface $-d$, por lo que si d es el máximo común divisor de a y b, también lo es $-d$, cuestión de no unicidad que obviamos en la misma definición, quedándonos siempre con el de valor no negativo, esto es,

$$0 \leq \mathrm{mcd}(a, b) = \mathrm{mcd}(-a, b) = \mathrm{mcd}(a, -b) = \mathrm{mcd}(-a, -b) = \mathrm{mcd}(|a|, |b|);$$

en realidad, el máximo común divisor se define en un dominio de integridad y en ese ámbito decimos que a y b son *elementos asociados* —o simplemente asociados— si, y sólo si, $a \mid b$ y $b \mid a$, pudiendo obtenerse resultados de «unicidad (salvo asociados)»); de todo ello, que en textos aparezca la condición 1.ª como esencial y las otras se sustituyan por la exigencia de que el $\mathrm{mcd}(a, b)$ es, de los divisores comunes, el mayor en valor absoluto, resumiéndose la 0.ª y 2.ª, por ejemplo, en que si $d' \mid a$ y $d' \mid b$, entonces $d' \leq d$.

Observación 18.3.4.— En cuanto a la notación, en vez de $\mathrm{mcd}(a, b)$, pudiésemos usar $\backslash a, b /$, o bien $\diagdown a, b \diagup$ —ésta está inspirada en la propuesta por Küster [204]— (*vid. et. infra* observación 18.3.5 (pág. 969 de esta edición).).

§ 18.3.1 Identidad y coeficientes de Bézout

La *identidad de* Bézout asegura que es posible representar el máximo común divisor de a y b como combinación lineal entera de a y b, si bien dicha representación no es única.

Teorema 18.28 (Identidad de Bézout)
Dados a y b con $\mathrm{mcd}(a, b) = d$, existen enteros s y t tales que $as + bt = d$; los enteros s y t, que no son únicos, se conocen como *coeficientes de* Bézout para a y b.

Teorema 18.29
Dados dos números enteros a y b, existen infinitos coeficientes de Bézout para ellos.

Demostración.— En efecto, dados unos coeficientes de Bézout determinados s_0 y t_0, esto es, si (s_0, t_0) es una solución de $as + bt = d$, con $d = \mathrm{mcd}(a, b)$, entonces $a(s - s_0) + b(t - t_0) = 0$, y así, la solución general es $(s, t) = (s_0 + bp, t_0 - ap)$, con $p \in \mathbb{Z}$. ■

Teorema 18.30
Si $a, b \in \mathbb{Z}$, entonces el *conjunto de múltiplos del* $\mathrm{mcd}(a, b)$ es $\{ka + hb : k, h \in \mathbb{Z}\}$.

§ 18.3.2 Propiedades del mcd como operación

Teorema 18.31
$\forall a, b, c \in \mathbb{Z}$, se satisface:

0. $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a)$, (conmutativa)
1. $\mathrm{mcd}\,(a, \mathrm{mcd}\,(b, c)) = \mathrm{mcd}\,(\mathrm{mcd}\,(a, b)\,, c)$; (asociativa)

por lo tanto, $\langle \mathbb{N}; \mathrm{mcd} \rangle$ y $\langle \mathbb{Z}; \mathrm{mcd} \rangle$ son *semigrupos abelianos*.

Observación 18.3.5.— Precisamente la asociatividad del mcd hace que Dijkstra proponga su notación infija (él usa $\downarrow$); de este modo, por ejemplo, las propiedades conmutativa y asociativa se escriben, respectivamente, $a \downarrow b = b \downarrow a$ y $a \downarrow (b \downarrow c) = (a \downarrow b) \downarrow c$.[28]

Teorema 18.32
$\forall a, b, c, d \in \mathbb{Z}$:

2. $\mathrm{mcd}(a, a) = |a|$
3. $\mathrm{mcd}(a, 0) = \mathrm{mcd}(0, a) = |a|$,
4. $\mathrm{mcd}(a, b) = \mathrm{mcd}(a, b - a)$ si $a \leq b$,
5. $\mathrm{mcd}(a, b) = \mathrm{mcd}(a - b, b)$ si $b \leq a$,
6. $\mathrm{mcd}(ca, cb) = |c|\,\mathrm{mcd}(a, b)$,
7. si $\mathrm{mcd}(a, b) = d$, entonces $\mathrm{mcd}(a/d, b/d) = 1$; (coprimidad)
8. $\mathrm{mcd}(a, 1) = \mathrm{mcd}(1, a) = 1$. (absorción)

Actividad 18.7

Llamando $m = \mathrm{mín}\{a, b\}$ y $M = \mathrm{máx}\{a, b\}$, demostremos que pudiésemos unificar 4 y 5 en

$$\mathrm{mcd}(m, M) = \mathrm{mcd}(m, M - m).$$

Actividad 18.8

[Cálculo del mcd, 0] Diseñemos una función que calcule recursivamente el máximo común divisor de dos números enteros. Optativamente, pudiésemos codificarla en Sage.

[28] Igualmente por ser asociativa la operación máximo, también propone Dijkstra su notación infija para la que usa $\uparrow$ (*vid. v. gr.* https://www.cs.utexas.edu/~EWD/transcriptions/EWD13xx/EWD1300.html).

Teorema 18.33

$\forall a \in \mathbb{N}$, se satisface:

9. $\text{mcd}(a, a) = a$, (idempotencia)
10. $\text{mcd}(a, 0) = \text{mcd}(0, a) = a$; (elemento neutro)

por lo tanto, $\langle \mathbb{N}; \text{mcd} \rangle$ es un *monoide abeliano idempotente*, ya que sabemos que $\langle \mathbb{N}; \text{mcd} \rangle$ es semigrupo abeliano.

Teorema 18.34

$\forall a, b, c \in \mathbb{Z}$, se satisface:

11. si $c \in \mathbb{N}$, $c \cdot \text{mcd}(a, b) = \text{mcd}(ca, cb)$ y $\text{mcd}(a, b) \cdot c = \text{mcd}(ac, bc)$; (distributiva de $\cdot$ respecto de mcd)

por lo tanto, $\langle \mathbb{N}; \text{mcd}, \cdot \rangle$ es un *semianillo abeliano aditivamente idempotente*, ya que sabemos que $\langle \mathbb{N}; \text{mcd} \rangle$ es monoide abeliano idempotente y $\langle \mathbb{N}; \cdot \rangle$ es semigrupo abeliano.

Observación 18.3.6.— Recordemos que un anillo es un semianillo en el que todo elemento tiene simétrico aditivo; en el caso de $\langle \mathbb{N}; \text{mcd}, \cdot \rangle$, la operación aditiva es mcd y, entonces, para ser anillo debería ocurrir que para todo natural a, existiera un natural a' tal que $\text{mcd}(a', a) = \text{mcd}(a, a') = 0$, cosa que no sucede.

Teorema 18.35 (Primos y mcd)

Si p es primo, entonces:

0. si $p \mid n$, $\text{mcd}(p, n) = p$, y si $p \nmid n$, $\text{mcd}(p, n) = 1$;
1. si $p \mid mn$, entonces $p \mid m$ o $p \mid n$ (en particular, si m y n son primos, entonces $p = m$ o $p = n$);
2. si $p \mid \prod_{i=0}^{k} n_i$, entonces p divide al menos a uno de los factores n_i (en particular, si todos los n_i son primos, entonces $p = n_i$ para algún índice i).

Ejemplo 527

¿Cuáles son los enteros positivos n, menores que 333, tales que $\text{mcd}(n, 396) = 33$?

[SEL 6:4]. *Cfr.* Prada y Rodríguez [205]: ejercicio 4.1.2 (pág. 33).

Resolución.— Observemos que $396 = 33 \cdot 12$. Tenemos que ingeniárnoslas para descubrir un método para hallar todos los números que nos piden. Un método, una estrategia, un algoritmo, imaginemos que fuesen números enormes, necesitaríamos la ayuda de la máquina y habría que implementarlo. Pensemos en $396 = 33 \cdot 12$, esa descomposición en factores puede ser un camino; pensemos también que es cierto que si $n = 33p$ y $\text{mcd}(12, p) = 1$, entonces $\text{mcd}(n, 396) = 33$.

¿Por qué $\text{mcd}(12, p) = 1$ (p coprimo con 12)? Esto forma parte de la estrategia que hemos diseñado. Porque $\text{mcd}(12, p) = 1$ (p coprimo con 12) unido a $n = 33p$, obliga a que sea cierto $\text{mcd}(n, 396) = 33$ —por la propiedad $\text{mcd}(ca, cb) = |c| \cdot \text{mcd}(a, b)$, en este caso, de $\text{mcd}(12, p) = 1$ se sigue $\text{mcd}(33 \cdot 12, 33p) = 33$—, que es lo que viene impuesto que tienen que satisfacer los n que buscamos (aparte de tener que ser menores que 333). Además, la elección $\text{mcd}(12, p) = 1$ (p coprimo con 12) y $n = 33p$ es apropiada para que no aumente el máximo común divisor, ya que $396 = 33 \cdot 2 \cdot 2 \cdot 3$.

Esto nos proporciona un procedimiento para descubrir los valores pedidos: dar valores a p con la condición de que son coprimos con 12 y ver qué resultados nos salen en $n = 33p$ que sean menores que 333.

Entonces, como los coprimos con 12 son $1, 5, 7, 11, \ldots$, calculamos los valores correspondientes de $n = 33p$:

- como $33 \cdot 1 = 33 < 333$, 33 es un resultado válido;
- como $33 \cdot 5 = 165 < 333$, 165 es un resultado válido;
- como $33 \cdot 7 = 231 < 333$, 231 es un resultado válido;
- como $33 \cdot 11 = 363 > 333$, 363 no es un resultado válido (y para $p > 11$, tampoco);

por lo tanto, los n pedidos son: 33, 165 y 231.

Como vemos, todo ha consistido en una reducción a un número finito y manejable de posibilidades, abordable por una demostración por casos, como hemos hecho.

Solución.— Los enteros positivos menores que 333, tales que $\text{mcd}(n, 396) = 33$, son 33, 165 y 231. ■

Actividad 18.9

Demostremos que $\sqrt{2}$ no es un número racional.

§ 18.3.3 Mutuamente primos y mutuamente coprimos

Definición 18.9 (Máximo común divisor de más de dos números).— $\text{mcd}(a, b, c) = \text{mcd}(a, \text{mcd}(b, c))$ e inductivamente, $d = \text{mcd}(a_0, a_1, \ldots, a_k) = \text{mcd}(a_0, \text{mcd}(a_1, \ldots, a_k))$, siendo cierto que d divide a cada a_i, que todo divisor común de los a_i divide a d y que d es combinación lineal de los a_i.

Definición 18.10.— Decimos que los números $a_0, a_1, \ldots, a_k$ son *primos entre sí* (o, sinónimamente, *mutuamente primos*), si, y sólo si, $\text{mcd}(a_0, a_1, \ldots, a_k) = 1$.

Definición 18.11.— Decimos que los números $a_0, a_1, \dots, a_k$ son *primos dos a dos* (o, sinónimamente, *mutuamente coprimos*) si, y sólo si, $\operatorname{mcd}(a_i, a_j) = 1$, $\forall i, j \in \mathbb{N}_{<k+1}$, con $i \neq j$.

Observación 18.3.7.— Si $k = 1$ ambas definiciones coinciden y diremos que a_0 y a_1 son *coprimos*, *primos relativos* o *primos entre sí*.

Observación 18.3.8.— Si $a_0, a_1, \dots, a_k$ son primos dos a dos, entonces son primos entre sí; el recíproco no es cierto, por ejemplo, 2, 3 y 4 son primos entre sí, pero no son primos dos a dos.

Observación 18.3.9.— Es sencillo obtener coprimos a partir de dos números; recordemos la propiedad de coprimidad estudiada: $a/\operatorname{mcd}(a, b)$ y $b/\operatorname{mcd}(a, b)$ son coprimos, esto es, $\operatorname{mcd}\left(a/\operatorname{mcd}(a, b), b/\operatorname{mcd}(a, b)\right) = 1$.

Teorema 18.36

Siendo $ab \neq 0$, $a, b \in \mathbb{Z}$ son coprimos si, y sólo si, existen $k, h \in \mathbb{Z}$ tales que $ka + hb = 1$.

Teorema 18.37 (Lema de Euclides)

Si $n \mid ab$ y $\operatorname{mcd}(n, a) = 1$ entonces $n \mid b$, esto es, si un número entero divide al producto de dos números enteros y es coprimo con uno, entonces divide al otro.

Teorema 18.38

Dos números enteros positivos consecutivos cualesquiera son coprimos.

§ 18.3.4 Cálculo del mcd, I

Existen varias maneras de calcular el máximo común divisor. Estudiaremos algunas en este apartado y en el siguiente.

Teorema 18.39 (Obtención del $\operatorname{mcd}(a, b)$, I)

Se hallan los conjuntos de divisores positivos de a y de b, se calcula el conjunto intersección de ellos y entonces, el $\operatorname{mcd}(a, b)$ es el máximo entre los elementos de este último conjunto:

0.º se hallan $D(a)$ y $D(b)$;

1.º se determina $D(a) \cap D(b)$, y

2.º $\operatorname{mcd}(a, b) = \operatorname{máx}(D(a) \cap D(b))$.

Ejemplo 528

Demostremos que el máximo común divisor de 315 y 135 es 45.

Resolución.—

$$\begin{aligned} D(315) &= \{1, 3, 5, 7, 9, 15, 21, 35, 45, 63, 105, 315\}, \\ D(135) &= \{1, 3, 5, 9, 15, 27, 45, 135\}, \\ D(315) \cap D(135) &= \{1, 3, 5, 9, 15, 45\}, \\ \mathrm{mcd}(315, 135) &= \mathrm{máx}(D(315) \cap D(135)) = 45. \end{aligned}$$ ■

Teorema 18.40 (Obtención del $\mathrm{mcd}(a, b)$, II)
Dadas las descomposiciones en factores primos de los enteros positivos a y b, su máximo común divisor es el producto de los factores primos comunes, tomados en cada caso con el menor exponente; esto es, si $a = \prod_{i=0}^{\infty} p_i^{a_i}$ y $b = \prod_{i=0}^{\infty} p_i^{b_i}$, con $a_i, b_i \geq 0$, entonces $\mathrm{mcd}(a, b) = \prod_{i=0}^{\infty} p_i^{c_i}$ con $c_i = \mathrm{mín}\{a_i, b_i\}$.

Ejemplo 529

Demostremos que el máximo común divisor de 315 y 135 es 45.

Resolución.—

$$\begin{aligned} 315 &= 3^2 \cdot 5 \cdot 7 \, (= 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot 11^0 \cdot \ldots), \\ 135 &= 3^3 \cdot 5 \, (= 2^0 \cdot 3^3 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot \ldots), \\ \mathrm{mcd}(315, 135) &= 3^{\mathrm{mín}\{2,3\}} \cdot 5^{\mathrm{mín}\{1,1\}} = 3^2 \cdot 5 = 45. \end{aligned}$$ ■

Ejemplo 530

Supongamos que el número de divisores positivos de $n \in \mathbb{Z}^+$ es 24 y que el máximo común divisor de todos los números que son posibles valores de n es 30. Hallemos todos estos números que son posibles valores de n.

[AIC 10.4.2019:7].

Resolución.— Como el máximo común divisor de todos los números posibles valores de n es 30 y $30 = 2 \cdot 3 \cdot 5$, se tiene que todos los posibles n tienen en común el producto $2^\alpha 3^\beta 5^\gamma m$, con $\alpha, \beta, \gamma \geq 1$. Como por hipótesis, $(\alpha + 1)(\beta + 1)(\gamma + 1)k = 24$ y, por otro lado, $24 = 2^3 \cdot 3 = 2 \cdot 3 \cdot 4$ y, por otro, $\alpha, \beta, \gamma \geq 1$, se tiene, necesariamente, que $k = 1$ y $\langle \alpha, \beta, \gamma \rangle$ es igual a $\langle 1, 2, 3 \rangle$ o a cualquier permutación de $\langle 1, 2, 3 \rangle$, y por lo tanto, los números posibles valores de n son los seis siguientes: $2 \cdot 3^2 \cdot 5^3$, $2 \cdot 3^3 \cdot 5^2$, $2^2 \cdot 3 \cdot 5^3$, $2^2 \cdot 3^3 \cdot 5$, $2^3 \cdot 3 \cdot 5^2$ y $2^3 \cdot 3^2 \cdot 5$. ■

§ 18.3.5 Cálculo del mcd, II: el algoritmo de Euclides

El algoritmo de EUCLIDES (300 a. C., *Elementos*, Libro VII) se basa en la siguiente caracterización y teorema.

Definición 18.12 (Caracterización de $|$ en términos del mcd).— $a \mid b$ si, y sólo si, $\text{mcd}(a, b) = |a|$.

Teorema 18.41 (Reducción de EUCLIDES)
$\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}^+$, si $a > b$ y si $a \nmid b$ y si $b \nmid a$ y si $a = bq + r$, con $0 \leq r < |b|$, entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$, reduciéndose así el problema inicial a uno de menor complejidad, al menos en cuanto a la magnitud de los números implicados.

El siguiente teorema nos muestra ya el algoritmo.

Teorema 18.42 (Algoritmo de EUCLIDES —obtención del mcd, III—)
Siendo $a, b \in \mathbb{Z}^+$ y $a > b$,
se divide a entre b, $a = bq_0 + r_0$, con $0 \leq r_0 < b$, entonces,
si $r_0 = 0$, $\text{mcd}(a, b) = b$, FIN;
si $r_0 \neq 0$, $\text{mcd}(a, b) = \text{mcd}(b, r_0)$,
se divide b entre r_0, $a = bq_1 + r_1$, con $0 \leq r_1 < r_0$, entonces,
si $r_1 = 0$, $\text{mcd}(b, r_0) = r_0$, FIN;
si $r_1 \neq 0$, $\text{mcd}(b, r_0) = \text{mcd}(r_0, r_1)$,
se divide r_0 entre $r_1, \ldots$
obteniéndose así una secuencia estrictamente decreciente de restos, $r_0 > r_1 > r_2 > \ldots > r_{k-1} > r_k > r_{k+1} = 0$, por lo que

$$\begin{aligned}
\text{mcd}(a, b) &= \text{mcd}(b, r_0) \\
&= \text{mcd}(r_0, r_1) \\
&= \text{mcd}(r_1, r_2) \\
&\vdots \\
&= \text{mcd}(r_{k-2}, r_{k-1}) \\
&= \text{mcd}(r_{k-1}, r_k) \\
&= \text{mcd}(r_k, r_{k+1}) \\
&= \text{mcd}(r_k, 0) \\
&= r_k
\end{aligned}$$

FIN.

Observación 18.3.10 (Implementación del algoritmo de EUCLIDES).— Dados $a, b \in \mathbb{Z}^+$ y $a > b$:

$$\begin{aligned} r_0 &\hookleftarrow a \\ r_1 &\hookleftarrow b \\ &\vdots \\ r_{i+1} &\hookleftarrow r_{i-1} - q_{i-1}r_i \qquad 0 \leq r_{i+1} < r_i \\ &\vdots \end{aligned}$$

que finaliza cuando se alcance un resto nulo $r_{k+1} = 0$, siendo entonces $\operatorname{mcd}(a, b) = r_k$ (el último resto no nulo).

Actividad 18.10

Como la secuencia de restos es monótona decreciente y está acotada inferiormente por cero, es una secuencia finita. Pero, ¿por qué se alcanza necesariamente un resto nulo?

Ejemplo 531

Demostremos que el máximo común divisor de 4947 y 1455 es 291 y calculemos los coeficientes de BÉZOUT s y t asociados a 4947 y 1455, respectivamente.

Resolución.—

Cálculo del máximo común divisor.

En efecto, la ejecución de la implementación del algoritmo de EUCLIDES es

	$q_0 = 3$	$q_1 = 2$	$q_2 = 2$
$a(= r_0) = 4947$	$b(= r_1) = 1455$	582	291
$r_2 = 582$	$r_3 = 291$	$r_4 = 0$	

siendo $r_2 > r_3 > r_{3+1} = 0$, luego

$$\operatorname{mcd}(4947, 1455) = \operatorname{mcd}(4947, 582) = \operatorname{mcd}(582, 291) = 291.$$

Cálculo de los coeficientes de BÉZOUT.

Por una parte, el desarrollo del cálculo del $\operatorname{mcd}(4947, 1455)$ es

$$\begin{aligned} 4947 &= 3 \cdot 1455 + 582, \\ 1455 &= 2 \cdot 582 + 291, \\ 582 &= 2 \cdot 291 + 0; \end{aligned}$$

por otra, recorriendo hacia atrás el cálculo anterior a partir del valor hallado para mcd(4947, 1455) (*sustitución regresiva* con objetivo la identidad de Bézout),

$$\begin{aligned}291 &= 1455 - 2 \cdot 582,\\ &= 1455 - 2(4947 - 3 \cdot 1455),\\ &= 7 \cdot 1455 + (-2) \cdot 4947,\\ &= (-2) \cdot 4947 + 7 \cdot 1455,\end{aligned}$$

en otras palabras,

$$\langle s, t \rangle = \langle -2, 7 \rangle.$$

■

Actividad 18.11

Pensemos en la ejecución del algoritmo de EUCLIDES para calcular el mcd(a, b) con $a > b$. Demostremos que:

0. el producto de los números iniciales a y b que intervienen en la reducción de EUCLIDES es mayor o igual que 1;
1. en la reducción de EUCLIDES, el producto del par de números final (b, r) es menor que la mitad del producto del par de números inicial (a, b), esto es, $br < ab/2$, esto es, en cada iteración del algoritmo de EUCLIDES, el producto del divisor por el resto es menor que la mitad del producto del dividendo por el divisor de la iteración anterior;
2. el producto del dividendo por el divisor correspondientes a la iteración i del algoritmo de EUCLIDES es menor que $ab/2^i$;
3. el número k de pasos del algoritmo de EUCLIDES es menor o igual que $\log_2 a + \log_2 b$.

[SEP 12.5.2022:5].

§ 18.3.6 Cálculo del mcd, III: el algoritmo de Euclides extendido

El *algoritmo de EUCLIDES extendido (AEE)* calcula el máximo común divisor de dos números y los coeficientes de BÉZOUT asociados. La implementación siguiente calcula el mcd(a, b) y los coeficientes de BÉZOUT s y t, dados $a, b \in \mathbb{Z}^+$ y $a > b$.

$$\begin{aligned}
r_0 &\hookleftarrow a & r_1 &\hookleftarrow b\\
s_0 &\hookleftarrow 1 & s_1 &\hookleftarrow 0\\
t_0 &\hookleftarrow 0 & t_1 &\hookleftarrow 1\\
&\vdots & &\vdots\\
r_{i+1} &\hookleftarrow r_{i-1} - q_{i-1} r_i & 0 &\leq r_{i+1} < r_i\\
s_{i+1} &\hookleftarrow s_{i-1} - q_{i-1} s_i & &\\
t_{i+1} &\hookleftarrow t_{i-1} - q_{i-1} t_i & &
\end{aligned}$$

$\vdots$

que finaliza cuando se alcance un resto nulo, digamos que r_{k+1} es 0, siendo entonces: 0.º, $\operatorname{mcd}(a, b)$ el último resto no nulo, es decir, $\operatorname{mcd}(a, b)$ es r_k; 1.º, s es s_k, y 2.º, t es t_k; en definitiva, $\operatorname{mcd}(a, b)$ es r_k y también es $as_k + bt_k$.

Observación 18.3.11.— El algoritmo de EUCLIDES extendido siempre genera uno de los pares minimales de coeficientes de BÉZOUT en el sentido de que satisfagan $|s| \leq |b/\operatorname{mcd}(a, b)|$ y $|t| \leq |a/\operatorname{mcd}(a, b)|$; esto es, hay infinitos coeficientes de BÉZOUT y AEE calcula los que satisfacen esa condición de minimalidad (ser menores o iguales que esos cocientes) independientemente del signo; de hecho, AEE también permite calcular esos cocientes: si $r_{k+1} = 0$, entonces $s_{k+1} = b/\operatorname{mcd}(a, b)$ y $t_{k+1} = a/\operatorname{mcd}(a, b)$.

Ejemplo 532

Demostremos que el máximo común divisor de 4947 y 1455 es 291.

Resolución.— Sigamos lo que dice el algoritmo de EUCLIDES extendido. Los pasos $i = 0$ e $i = 1$ son de inicialización de variables: $r_0 = 4947$, $s_0 = 1$, $t_0 = 0$, $r_1 = 1455$, $s_1 = 0$, $t_1 = 1, \ldots$

i	q_{i-1}	r_i	s_i	t_i
0		4947	1	0
1		1455	0	1
2	$4947 \operatorname{div} 1455 = 3$	$4947 - 3 \cdot 1455 = 582$ $(= 4947 \operatorname{mód} 1455)$	$1 - 3 \cdot 0 = 1$	$0 - 3 \cdot 1 = -3$
3	$1455 \operatorname{div} 582 = 2$	$1455 - 2 \cdot 582 = 291$ $(= 1455 \operatorname{mód} 582)$	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot (-3) = 7$
4	$582 \operatorname{div} 291 = 2$	$582 - 2 \cdot 291 = 0$ $(= 582 \operatorname{mód} 291)$	$1 - 2 \cdot (-2) = 5$	$(-3) - 2 \cdot 7 = -17$

Recordemos la notación que usamos: si $a = bq + r$, entonces $a \operatorname{div} b = q$ y $a \operatorname{mód} b = r$. Así, como $r_4 = 0$, $r_3 = 291$ es el $\operatorname{mcd}(4947, 1455)$ y $s_3 = -2$ y $t_3 = 7$ son los coeficientes de BÉZOUT asociados a 4947 y a 1455, respectivamente, esto es, $291 = (-2) \cdot 4947 + 7 \cdot 1455$. Además, $|s_4| = b/\operatorname{mcd}(a, b)$ y $|t_4| = a/\operatorname{mcd}(a, b)$, esto es, $|s_4| = 5 = 1455/291$ y $|t_4| = 17 = 4947/291$. Los números $|s_4|$ y $|t_4|$ son los valores de $|b/\operatorname{mcd}(a, b)|$ y $|a/\operatorname{mcd}(a, b)|$, respectivamente. Esto es lo que dijimos anteriormente, que $|s_3| \leq |s_4|$ y que $|t_3| \leq |t_4|$ (se darían las igualdades si a fuese múltiplo de b —estamos suponiendo $a > b$—). ■

§ 18.3.7 Mínimo común múltiplo

Definición 18.13.— Llamamos *múltiplo común* de a y b a cualquier número que sea múltiplo de a y de b.

Teorema 18.43 (de existencia y unicidad del mínimo común múltiplo)
Dados dos números a y b, existe un número m, y sólo uno, que satisface:
0.º $m \geq 0$ (m es no negativo);
1.º $a \mid m$ y $b \mid m$ (m es un múltiplo común de a y de b), y
2.º si $a \mid m'$ y $b \mid m'$, entonces $m \mid m'$) (todo múltiplo común de a y de b es múltiplo de m);
el único m en esas condiciones se denomina *mínimo común múltiplo* de a y b y se designa por $\operatorname{mcm}(a, b)$, aMb o simplemente $[a, b]$.

En realidad, también pudiésemos usar la notación $/a, b\backslash$, o bien $\diagup a, b \diagdown$. Ésta está inspirada en Küster [204].

Observación 18.3.12.— $\operatorname{mcm}(a, b) = 0$ si, y sólo si, $a = 0$ y $b = 0$; en cualquier otro caso, $\operatorname{mcm}(a, b) \geq 1$.

Observación 18.3.13.— Notemos que si $\operatorname{mcm}(a, b) = m$ también lo es $-m$, cuestión que obviamos quedándonos, por definición, siempre con el de valor no negativo, esto es,

$$0 \leq \operatorname{mcm}(a, b) = \operatorname{mcm}(-a, b) = \operatorname{mcm}(a, -b) = \operatorname{mcm}(-a, -b) = \operatorname{mcm}(|a|, |b|);$$

en realidad, el mcm se define en un dominio de integridad y en ese ámbito decimos que a y b son *elementos asociados* —o simplemente asociados— si, y sólo si, $a \mid b$ y $b \mid a$, pudiendo obtenerse resultados de «unicidad (salvo asociados)»); de todo ello, que en textos aparezca la condición 1.ª como esencial y las otras se sustituyan por la exigencia de que el $\operatorname{mcm}(a, b)$ es, de los múltiplos comunes, el menor en valor absoluto, resumiéndose la 0.ª y 2.ª, por ejemplo, en que si $a \mid m'$ y $b \mid m'$, entonces $m \leq m'$.

Teorema 18.44 (de redefinición de | en términos del mcm)
$\forall a, b, c \in \mathbb{Z}$: $a \mid b$ si, y sólo si, $\operatorname{mcm}(a, b) = |b|$.

§ 18.3.8 Propiedades del mcm como operación

Teorema 18.45

$\forall a, b, c \in \mathbb{Z}$, se satisface:

0. $\operatorname{mcm}(a,b) = \operatorname{mcm}(b,a)$; (conmutativa)
1. $\operatorname{mcm}(a, \operatorname{mcm}(b,c)) = \operatorname{mcm}(\operatorname{mcm}(a,b), c)$; (asociativa)

por lo tanto, $\langle \mathbb{N}; \operatorname{mcm}\rangle$ y $\langle \mathbb{Z}; \operatorname{mcm}\rangle$ son *semigrupos abelianos*.

Teorema 18.46

$\forall a, b, c, d \in \mathbb{Z}$:

2. $\operatorname{mcm}(a,a) = |a|$
3. $\operatorname{mcm}(a,1) = \operatorname{mcm}(1,a) = |a|$;
4. $\operatorname{mcm}(ca, cb) = |c| \operatorname{mcm}(a,b)$;
5. $\operatorname{mcm}(a,0) = \operatorname{mcm}(0,a) = 0$. (absorción)

Teorema 18.47

$\forall a \in \mathbb{N}$, se satisface:

6. $\operatorname{mcm}(a,a) = a$; (idempotencia)
7. $\operatorname{mcm}(a,1) = \operatorname{mcm}(1,a) = a$; (elemento neutro)

por lo tanto, $\langle \mathbb{N}; \operatorname{mcm}\rangle$ es un *monoide abeliano idempotente*, ya que sabemos que $\langle \mathbb{N}; \operatorname{mcm}\rangle$ es semigrupo abeliano.

Teorema 18.48

$\forall a, b, c \in \mathbb{Z}$, se satisface:

8. si $c \in \mathbb{N}$, $c \cdot \operatorname{mcm}(a,b) = \operatorname{mcm}(ca, cb)$ y $\operatorname{mcm}(a,b) \cdot c = \operatorname{mcm}(ac, bc)$; (distributiva de $\cdot$ respecto de mcm)

por lo tanto, $\langle \mathbb{N}; \operatorname{mcm}, \cdot\rangle$ es un *semianillo abeliano aditivamente idempotente*, ya que sabemos que $\langle \mathbb{N}; \operatorname{mcm}\rangle$ es monoide abeliano idempotente y $\langle \mathbb{N}; \cdot\rangle$ es semigrupo abeliano.

§ 18.3.9 Cálculo del mcm

Definición 18.14 (mínimo común múltiplo de más de dos números).— $\operatorname{mcm}(a,b,c) = \operatorname{mcm}(a, \operatorname{mcd}(b,c))$ e inductivamente, $m = \operatorname{mcm}(a_0, a_1, \ldots, a_k) = \operatorname{mcm}(a_0, \operatorname{mcm}(a_1, \ldots, a_k))$, siendo cierto que m es múltiplo de cada a_i y que m divide a cualquier múltiplo común de los a_i.

Teorema 18.49 (coprimos y mcm)

Si $\operatorname{mcd}(a,b) = 1$, entonces $\operatorname{mcm}(a,b) = ab$.

Teorema 18.50 (Obtención del $\text{mcm}(a, b)$, I)
Un primer algoritmo de cálculo del mcm es el siguiente.

0.º Hallamos $M(a)$ y $M(b)$ y
1.º determinamos $M(a) \cap M(b)$, entonces
2.º $\text{mcm}(a, b) = \text{mín}(M(a) \cap M(b))$.

Teorema 18.51 (Obtención del $\text{mcm}(a, b)$, II)
Un segundo algoritmo de cálculo del mcm es el siguiente: dadas las descomposiciones en factores primos de a y b, $\text{mcm}(a, b)$ es el producto de todos los factores primos tomando los comunes con el mayor exponente; esto es,

$$\text{si } a = \prod_{i=0}^{\infty} p_i^{a_i} \text{ y } b = \prod_{i=0}^{\infty} p_i^{b_i}, \text{ con } a_i, b_i \geq 0, \text{ entonces } \text{mcd}(a, b) = \prod_{i=0}^{\infty} p_i^{\text{máx}\{a_i, b_i\}}.$$

Teorema 18.52 (Obtención del $\text{mcm}(a, b)$, III)
Un tercer algoritmo de cálculo del mcm surge del hecho de que $(\forall a, b \in \mathbb{Z})$ $(\text{mcd}(a, b) \cdot \text{mcm}(a, b) = |a \cdot b|)$, en concreto:

$$\text{mcm}(a, b) = \begin{cases} |a \cdot b| / \text{mcd}(a, b) & \text{si } a \neq 0 \wedge b \neq 0 \\ 0 & \text{si } a = 0 \vee b = 0. \end{cases}$$

§ 18.3.10 Propiedades conjuntas del mcd y mcm como operaciones

Teorema 18.53 (Propiedades conjuntas del mcd y mcm como operaciones)
$\forall a, b, c \in \mathbb{Z}$:

0. $\text{mcd}(a, \text{mcm}(a, b)) = \text{mcm}(a, \text{mcd}(a, b)) = |a|$ (absorción)
1. si $a \in \mathbb{N}$, entonces $\text{mcd}(a, \text{mcm}(a, b)) = \text{mcm}(a, \text{mcd}(a, b)) = a$; (absorción)
2. $\text{mcd}(a, \text{mcm}(b, c)) = \text{mcm}(\text{mcd}(a, b), \text{mcd}(a, c))$; (distributiva del mcd en el mcm)
3. $\text{mcm}(a, \text{mcd}(b, c)) = \text{mcd}(\text{mcm}(a, b), \text{mcm}(a, c))$; (distributiva del mcm en el mcd)
4. $\text{mcd}(a, b) = \text{mcd}(a + b, \text{mcm}(a, b))$;
5. $\langle \mathbb{Z}^+; \text{mcd}, \text{mcm}, 0, 1 \rangle$ es un *retículo distributivo y acotado*.

Observación 18.3.14.— Como no es cierto que para todo $a \in \mathbb{Z}^+$, exista $a' \in \mathbb{Z}^+$ tal que $\text{mcd}(a, a') = 1$ y $\text{mcm}(a, a') = 0$, entonces $\langle \mathbb{Z}^+; \text{mcd}, \text{mcm}, 0, 1 \rangle$ no es un retículo complementado y por tanto no es un álgebra de Boole (ya que ésta es un retículo distributivo y complementado

—y, por tanto, acotado—). Notemos, por ejemplo, la analogía con el álgebra de Boole $\langle 2^X; \cup, \cap, \emptyset, X\rangle$, donde sí se da la existencia, para todo A de 2^X, de $A^{\complement} \in 2^X$ tal que $A \cup A^{\complement} = X$ y $A \cap A^{\complement} = \emptyset$.

Actividad 18.12

A propósito de álgebra de Boole, pensemos en el conjunto de los divisores positivos de 30: $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$, en el que los papeles de las operaciones entre conjuntos, unión e intersección, los jueguen, respectivamente, las operaciones entre números, mínimo común múltiplo y máximo común divisor, siendo la correspondiente a la complementariedad, para un número a, la operación $30/a$, y 1 y 30 los correspondientes al conjunto vacío y al universal en el álgebra de Boole de los conjuntos; pues bien, $\langle D_{30}; \text{mcm}, \text{mcd}, 1, 30\rangle$ tiene estructura de álgebra de Boole.[29]

§ 18.4 Funciones aritméticas

Definición 18.15.— Llamamos *función aritmética* a cualquier función real o compleja definida en $\mathbb{Z}^+$.

Definición 18.16.— Llamamos *función multiplicativa* a toda función aritmética f distinta de la función cero y tal que $\forall m, n \in \mathbb{Z}^+$, si $\text{mcd}(m, n) = 1$, entonces $f(mn) = f(m) \cdot f(n)$.

Definición 18.17.— Llamamos *función completamente multiplicativa* a toda función multiplicativa tal que $(\forall m, n \in \mathbb{Z}^+)(f(mn) = f(m) \cdot f(n))$.

Definición 18.18.— Definimos la *multiplicación de* Dirichlet de dos funciones aritméticas f y g como

$$(f * g)(n) = \sum_{\substack{a \cdot b = n \\ a, b > 0}} f(a)g(b).$$

[29] Observemos que $2 \cdot 3 \cdot 5 = 30$ y que $D_{30} \setminus \{1\}$ está generado por los primos 2, 3 y 5 y las operaciones mcm y mcd; por otra parte, los primos 2, 3, 5 y 7 ($2 \cdot 3 \cdot 5 \cdot 7 = 210$) y las operaciones mcm y mcd generan $D_{210} \setminus \{1\}$, siendo $\langle D_{210}; \text{mcm}, \text{mcd}, 1, 210\rangle$ un álgebra de Boole en la que la operación complementario de un número a es $210/a$; en realidad, el conjunto correspondiente generado por n primos distintos, uniéndole el 1, con las operaciones correspondientes mencionadas tiene estructura de álgebra de Boole, siendo 1 y el producto de dichos primos los correspondientes al conjunto vacío y al universal en el álgebra de Boole de los conjuntos (*vid. v. gr.* Reuben Louis Goodstein, *Boolean Algebra*, Dover, 2007, 2.8 y ejemplo II.10: *N is a product of n distinct primes $p_1, p_2, \ldots, p_n$ and $a, b, c, \ldots$ are the various divisors of N (including unity); $a \cup b$ is the least common multiple of a, b and $a \cap b$ is their highest common factor. If 0 has the value unity and 1 the value N, and if $a' = N/a$, prove that the relations 2.01–2.04 [definición de álgebra de* Boole*] are all satisfied by $a, b, c, \ldots$*).

Teorema 18.54 (Propiedades de estructura de la multiplicación de DIRICHLET)
El conjunto de las funciones aritméticas f tales que $f(1) \neq 0$ con la operación producto de DIRICHLET tiene estructura de *grupo abeliano*, esto es, $\forall f, g, h$ funciones aritméticas:

0. $f * g = g * f$; (conmutativa)
1. $(f * g) * h = f * (g * h)$; (asociativa)
2. $I * f = f * I = f$, siendo I la función identidad, completamente multiplicativa, definida por $I(n) = 1$ si $n = 1$ e $I(n) = 0$ si $n > 1$; (neutro)
3. si f es tal que $f(1) \neq 0$, entonces existe f^{-1} (*inversa de* DIRICHLET) tal que $f^{-1} * f = f * f^{-1} = I$, concretamente definida por
$$f^{-1}(n) = \begin{cases} 1 & \text{si } n = 1 \\ \frac{-1}{f(1)} \sum\limits_{\substack{d \mid n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) & \text{si } 1 < n. \end{cases} \qquad \text{(simétrico)}$$

Teorema 18.55 (Propiedades multiplicativas de la multiplicación de DIRICHLET)
$\forall f, g, h$ funciones aritméticas:

0. si f y g son multiplicativas, entonces $f * g$ es multiplicativa;
1. si f es multiplicativa, también lo es f^{-1}, su inversa de DIRICHLET;
(por tanto, el conjunto de las funciones multiplicativas es un *subgrupo* del grupo abeliano de las funciones aritméticas f tales que $f(1) \neq 0$).

§ 18.4.0 Función de MÖBIUS

Definición 18.19.— La *función de* MÖBIUS, $\mu(n)$, está definida por
$$\mu(1) = 1$$
y si $n = p_0^{\alpha_0} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, por
$$\mu(n) = \begin{cases} (-1)^k & \text{si } \alpha_0 = \alpha_1 = \ldots = \alpha_k = 1, \\ 0 & \text{en otro caso.} \end{cases}$$

Observación 18.4.0.— $\mu(n) = 0$ si, y sólo si, n tiene un divisor cuadrado mayor que 1.

Teorema 18.56
$$\sum_{d \in D(n)} \mu(d) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases}$$

Teorema 18.57
μ es multiplicativa pero no completamente multiplicativa.

§ 18.4.1 Función indicatriz de Euler

Definición 18.20.— El valor de la *función indicatriz de* Euler, $\varphi(n)$, para todo $n \in \mathbb{Z}^+$, es el número de enteros positivos menores que n que son primos con n, es decir, designando por $t(n)$ al conjunto $\{k \in \mathbb{Z}^+, 1 \leq k < n,\ \text{mcd}(k,n) = 1\}$, entonces $\varphi(n) = |t(n)|$; convenimos en que $\varphi(1) = 1$.

Ejemplo 533

Calculemos los valores de φ para los primeros diez números enteros positivos.

Resolución.— Calculémoslos por definición de φ, por ejemplo, menores que 4 y primos con 4 sólo hay dos, el 1 y el 3, por eso, $\varphi(4) = 2$. Éstos son:

$$\begin{aligned}
\varphi(1) &= 1 \text{ (por convenio)},\\
\varphi(2) &= |\{1\}| = 1,\\
\varphi(3) &= |\{1,2\}| = 2,\\
\varphi(4) &= |\{1,3\}| = 2,\\
\varphi(5) &= |\{1,2,3,4\}| = 4,\\
\varphi(6) &= |\{1,5\}| = 2,\\
\varphi(7) &= |\{1,2,3,4,5,6\}| = 6,\\
\varphi(8) &= |\{1,3,5,7\}| = 4,\\
\varphi(9) &= |\{1,2,4,5,7,8\}| = 6,\\
\varphi(10) &= |\{1,3,7,9\}| = 4.
\end{aligned}$$

■

Observación 18.4.1.— En inglés, $\varphi(n)$ es la Euler *totient function* y cada $k \in t(n)$ es un *totative* (o, sinónimamente, *totitive*) de n. Por ejemplo, 1, 3, 5, y 7 son los *totatives* de 8.

Teorema 18.58 (Primeras propiedades de φ)
$\forall p \in \mathbb{Z}^+$, p primo,

0. $\varphi(p) = p - 1$;
1. $\forall \alpha \in \mathbb{Z}^+, \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha \left(1 - \dfrac{1}{p}\right)$.

Teorema 18.59 (φ es una función multiplicativa)
Se satisface:

0. $\forall m, n \in \mathbb{Z}^+$, si $\operatorname{mcd}(m, n) = 1$, entonces $\varphi(mn) = \varphi(m) \cdot \varphi(n)$;
1. $\forall n_0, n_1, \ldots, n_k \in \mathbb{Z}^+$, si $\operatorname{mcd}(n_0, n_1, \ldots, n_k) = 1$, entonces $\varphi(n_0 n_1 \cdots n_k) = \varphi(n_0)\varphi(n_1) \cdots \varphi(n_k)$.

Teorema 18.60 ($\varphi(n)$ y la descomposición en factores primos de n)
Para todo entero positivo n,

$$\varphi(n) = n \prod_{\substack{p \mid n \\ p \text{ primo}}} \left(1 - \frac{1}{p}\right),$$

Demostración.— Sea $n = p_0^{\alpha_0} \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$; en la siguiente cadena de igualdades apreciamos diversas expresiones que nos permitirán hallar $\varphi(n)$ (en realidad, **algoritmos para calcular $\varphi(n)$**):

$$\begin{aligned}
\varphi(n) &= \varphi\left(p_0^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) \\
&= \varphi\left(p_0^{\alpha_0}\right) \varphi\left(p_1^{\alpha_1}\right) \cdots \varphi\left(p_k^{\alpha_k}\right) \\
&= p_0^{\alpha_0 - 1}\left(p_0 - 1\right) p_1^{\alpha_1 - 1}\left(p_1 - 1\right) \cdots p_k^{\alpha_k - 1}\left(p_k - 1\right) \\
&= p_0^{\alpha_0 - 1} p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}\left(p_0 - 1\right)\left(p_1 - 1\right) \cdots \left(p_k - 1\right) && (18.0) \\
&= p_0^{\alpha_0}\left(1 - \frac{1}{p_0}\right) p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) && (18.1) \\
&= n \cdot \left(1 - \frac{1}{p_0}\right) \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right), && (18.2)
\end{aligned}$$

por, ejemplo, observemos el algoritmo 18.1 en función de los factores primarios y de los complementos a uno de los recíprocos de los primos correspondientes, fácil de recordar. ■

Ejemplo 534

Calculemos $\varphi(60)$ y $\varphi(318)$.

Resolución.— Veamos, utilizando el algoritmo 18.2:

- de ser $60 = 2^2 \cdot 3 \cdot 5$, se sigue que $\varphi(60) = 60 \cdot (1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/5) = 16$, y
- como $318 = 2 \cdot 3 \cdot 53$, $\varphi(318) = 318 \cdot (1 - 1/2) \cdot (1 - 1/3) \cdot (1 - 1/53) = 104$. ■

Teorema 18.61 (φ no es completamente multiplicativa)
$(\forall m, n \in \mathbb{Z}^+)(\operatorname{mcd}(m, n) = d \rightarrow \varphi(mn) = \varphi(m)\varphi(n)d/\varphi(d))$.

Teorema 18.62 (Otras propiedades de φ)

Se satisface:

0. $(\forall d, n \in \mathbb{Z}^+)(d \mid n \to \varphi(d) \mid \varphi(n))$;
1. $(\forall n \in \mathbb{Z}^+)$ (si $n \geq 3$, entonces $\varphi(n)$ es par);
2. $(\forall n \in \mathbb{Z}^+)\left(n = \sum_{d \in D(n)} \varphi(d)\right)$.

Teorema 18.63 (Relación entre μ y φ)

$$(\forall n \in \mathbb{Z}^+)\left(\varphi(n) = \sum_{d \in D(n)} \mu(d)\frac{n}{d}\right).$$

Ejemplo 535

Utilicemos el teorema 18.62.0 (pág. 985 de esta edición) para calcular $\varphi(60)$.

Resolución.— Utilizando el algoritmo 18.0:

$$\begin{aligned}
\varphi(60) &= \varphi(2^2 \cdot 3 \cdot 5)\\
&= \varphi(2^2) \cdot \varphi(3) \cdot \varphi(5)\\
&= 2^{2-1} \cdot 3^{1-1} \cdot 5^{1-1} \cdot (2-1) \cdot (3-1) \cdot (5-1)\\
&= 2^1 \cdot 3^0 \cdot 5^0 \cdot 1 \cdot 2 \cdot 4\\
&= 16
\end{aligned}$$



Ejemplo 536

Utilicemos el teorema 18.58.0 (pág. 983 de esta edición) y el teorema 18.62.2 (pág. 985 de esta edición) para calcular $\varphi(318)$.

Resolución.— Basémonos en los valores de φ para todas las partes alícuotas de 318. Usemos el teorema 18.62.2 (pág. 985 de esta edición). El rango del sumatorio indica recorrer todos los divisores positivos de 318, esto es, el conjunto $D(318) = \{1, 2, 3, 6, 53, 106, 159, 318\}$.

Entonces, por el teorema 18.62.2 (pág. 985 de esta edición),

$$318 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) + \varphi(53) + \varphi(106) + \varphi(159) + \varphi(318),$$

por lo que es posible calcular $\varphi(318)$ así:

$$\varphi(318) = 318 - \varphi(1) - \varphi(2) - \varphi(3) - \varphi(6) - \varphi(53) - \varphi(106) - \varphi(159).$$

Calculemos ahora todo lo que nos hace falta, $\varphi(53)$, $\varphi(106)$ y $\varphi(159)$.

Por el teorema 18.58.0 (pág. 983 de esta edición), como 53 es un número primo, $\varphi(53) = 53-1 = 52$ —otra forma de calcularlo pudiese ser usar el teorema 18.62.2 (pág. 985 de esta edición): como $D(53) = \{1, 53\}$, entonces $53 = \varphi(1) + \varphi(53)$, y así,

$$\begin{aligned}\varphi(53) &= 53 - \varphi(1)\\ &= 53 - 1\\ &= 52.\end{aligned}$$

Continuemos; nos quedan $\varphi(106)$ y $\varphi(159)$.

Como $D(106) = \{1, 2, 53, 106\}$, entonces, por el teorema 18.62.2 (pág. 985 de esta edición),

$$\begin{aligned}\varphi(106) &= 106 - \varphi(1) - \varphi(2) - \varphi(53)\\ &= 106 - 1 - 1 - 52\\ &= 52,\end{aligned}$$

y como $D(159) = \{1, 3, 53, 159\}$, entonces, por el teorema 18.62.2 (pág. 985 de esta edición):

$$\begin{aligned}\varphi(159) &= 159 - \varphi(1) - \varphi(3) - \varphi(53)\\ &= 159 - 1 - 2 - 52\\ &= 104,\end{aligned}$$

por tanto,

$$\begin{aligned}\varphi(318) &= 318 - \varphi(1) - \varphi(2) - \varphi(3) - \varphi(6) - \varphi(53) - \varphi(106) - \varphi(159)\\ &= 318 - 1 - 1 - 2 - 2 - 52 - 52 - 104\\ &= 104.\end{aligned}$$

■

Algoritmos para calcular $\varphi(n)$

Como hemos visto, las propiedades proporcionan algoritmos de cálculo de $\varphi(m)$. Si tuviésemos tiempo e inquietud, no estaría de más que investigásemos acerca de los diferentes *algoritmos para calcular* $\varphi(n)$. En cualquier caso, con sistemas no cuánticos de cómputo, para n grande, es computacionalmente imposible calcular

$\varphi(n)$; precisamente esta imposibilidad material de factorizar un número grande es uno de los puntos fuertes de la seguridad de la mayoría de los sistemas criptográficos actuales.

§ 18.4.2 Funciones divisor

Definición 18.21.— La *función divisor* $\sigma_\alpha(n)$ está definida, $\forall n \in \mathbb{Z}^+$, por

$$\sigma_\alpha(n) = \sum_{d \in D(n)} d^\alpha,$$

esto es, $\sigma_\alpha(n)$ es la suma de las potencias de exponentes α de los divisores positivos de n, siendo α un número real o complejo.

Por ejemplo:

- $\sigma_0(n)$ es el número de divisores positivos de n; esta función también suele designarse por $d(n)$, $\upsilon(n)$ o $\tau(n)$; es conocida como la *función número de divisores*;
- $\sigma_1(n)$ es la suma de los divisores positivos de n; es conocida como la *función suma de divisores* y, frecuentemente, se omite el subíndice, esto es, $\sigma_1(n)$ suele notarse simplemente por $\sigma(n)$;
- $\sigma_2(n)$ es la suma de los cuadrados de los divisores positivos de n;
- $\sigma_3(n)$ es la suma de los cubos de los divisores positivos de n,

y así sucesivamente.

Teorema 18.64 (Propiedades de las funciones divisor)
Se satisface:

0. las funciones divisor son multiplicativas;
1. $(\forall n \in \mathbb{Z}^+)\left(\sigma_\alpha^{-1}(n) = \sum_{d \in D(n)} d^\alpha \mu(d) \mu\left(\frac{n}{d}\right)\right).$ (inversa de Dirichlet)

Definición 18.22.— La *función suma alícuota* $s(n)$ es la suma de las partes alícuotas de n, esto es,

$$s(n) = \sigma(n) - n.$$

Suele designarse también por $\sigma'(n)$.

Definición 18.23.— Llamamos *sucesión alícuota* de término inicial n a la sucesión de iteraciones de $s(n)$,

$$s^0(n) = n, s^1(n) = s(n), s^2(n) = s(s(n)), \ldots$$

Ejemplo 537

Calculemos $\sigma_0(12)$, $\sigma(12)$, $s(12)$ y la tupla de términos de la sucesión alícuota de término inicial 12.

Resolución.— Como $D(12) = \{1, 2, 3, 4, 6, 12\}$, entonces $\sigma_0(12) = |D(12)| = 6$, $\sigma(12) = \sigma_1(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$, $s(12) = \sigma(12) - 12 = 16$ y $\langle 12, 16, 15, 9, 4, 3, 1, 0\rangle$ (esta sucesión alícuota no tiene más términos[30]). ■

§ 18.5 Congruencias en el anillo de los enteros

Definición 18.24 (Gauss, 1801).— Decimos que a es *congruente* con b módulo m y notamos $a \equiv b \pmod{m}$, precisamente si dados $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$, sucede que

$$a \text{ mód } m = b \text{ mód } m,$$

esto es, al hacer sus divisiones enteras por m, sus *restos* (o, sinónimamente, *residuos*) son iguales. Llamamos *módulo* de la congruencia a m. Si a mód $m \neq b$ mód m escribimos $a \not\equiv b \pmod{m}$ y decimos que a y b son *incongruentes* módulo m.

Teorema 18.65

Dados $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$,

$$a \equiv b \pmod{m} \text{ si, y sólo si } m\,|\,(a - b).$$

Teorema 18.66

Dados $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$,

$$a \equiv b \pmod{m} \text{ si, y sólo si } (a - b) \equiv 0 \pmod{m}$$

(esto es, precisamente si a y b difieren en un múltiplo de m).

[30] *Vid. v. gr.* https://oeis.org/A044050 y https://mathworld.wolfram.com/AliquotSequence.html.

Teorema 18.67 (Propiedades de las congruencias como relación diádica)
$\forall a, b, c \in \mathbb{Z}, \forall m \in \mathbb{Z}^+$:

0. $a \equiv a \pmod{m}$; (reflexiva en $\mathbb{Z}$)
1. $a \equiv b \pmod{m} \to b \equiv a \pmod{m}$; (simétrica en $\mathbb{Z}$)
2. $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \to a \equiv c \pmod{m}$, (transitiva en $\mathbb{Z}$).

De acuerdo con este teorema, $\equiv \pmod{m}$ es una *relación diádica de equivalencia en* $\mathbb{Z}$.

En general, el conjunto cociente, $\mathbb{Z}/_{(\text{mod } m)}$, usualmente notado $\mathbb{Z}/_{m\mathbb{Z}}$ y abreviadamente $\mathbb{Z}_m$, es

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\},$$

cuyos elementos son las clases de equivalencia —*clases de residuos (o restos) módulo m*—:

$$\begin{aligned} 0 = [0]_m &= \{n \in \mathbb{Z} : n \equiv 0 \pmod{m}\} \\ &\vdots \\ m-1 = [m-1]_m &= \{n \in \mathbb{Z} : n \equiv m-1 \pmod{m}\}. \end{aligned}$$

Ejemplo 538

Imaginemos un reloj parlante cantando la hora: «Son 100 horas pasadas las 00 : 00». ¿Qué hora es?

[Cubit 128].

Resolución.— Ésta es la ecuación a resolver:

$$t \text{ mód } 24 = 100 \text{ mód } 24 \tag{18.3}$$

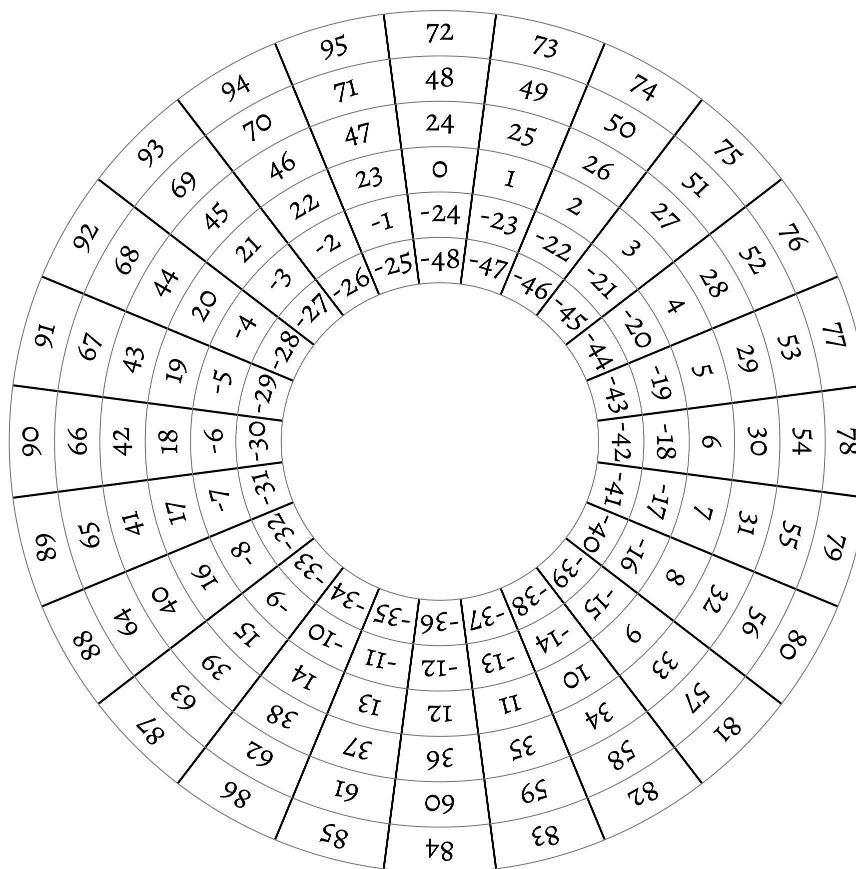
con $0 \leq t < 24$, esto es, t mód $24 = 4$, por tanto, $t = 4$, así que son las 4 horas.

Observemos que este reloj tiene 24 horas, desde la cero hasta la 23. Observemos también que:

- la hora cero es la misma que la hora $\ldots, -96, -72, -48, -24, 24, 48, 72, 96, \ldots$, esto es, $[0]_{24} = \{n \in \mathbb{Z} : n \equiv 0 \pmod{24}\} = \{0 \pm 24k : k \in \mathbb{Z}\}$;
- la hora uno es la misma que la hora $\ldots, -95, -71, -47, -23, 25, 49, 73, 97, \ldots$, esto es, $[1]_{24} = \{n \in \mathbb{Z} : n \equiv 1 \pmod{24}\} = \{1 \pm 24k : k \in \mathbb{Z}\}$;
- $\ldots$
- la hora cuatro es la misma que la hora $\ldots, -92, -68, -44, -20, 28, 52, 76, 100, \ldots$, esto es, $[4]_{24} = \{n \in \mathbb{Z} : n \equiv 4 \pmod{24}\} = \{4 \pm 24k : k \in \mathbb{Z}\}$;

- ...
- la hora veintitrés es la misma que la hora $\ldots, -97, -73, -49, -25, -1, 47, 71, 95, \ldots$, esto es, $[23]_{24} = \{n \in \mathbb{Z} : n \equiv 23 \pmod{24}\} = \{23 \pm 24k : k \in \mathbb{Z}\}$.

  La siguiente es una representación de este reloj.



En este ejemplo, el conjunto cociente es $\mathbb{Z}_{23} = \{[0], [1], \ldots, [23]\}$. En esta representación están todas estas clases de equivalencia y seis de sus elementos, por ejemplo, $[23] = \{\ldots, -25, -1, 47, 71, 95, \ldots\}$. ∎

Observación 18.5.0.— El número entero x mód m (el resto de la división euclidea, entre 0 y $|m|-1$, ambos inclusive) se conoce como la *representación positiva de x módulo m*. En realidad, para x, es el menor entero positivo en la clase $[x]_m$.

Suele hablarse también de la *representación positiva de $\mathbb{Z}_m$*. Es la que conocemos, por ejemplo, $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

También se trabaja con la *representación simétrica de x módulo m*, que es el número entero de la clase $[x]_m$ con menor valor absoluto, que notamos x móds m, hablándose también de la *representación simétrica de $\mathbb{Z}_m$*. Por ejemplo, $\mathbb{Z}_7 = \{-3, -2, -1, 0, 1, 2, 3\}$. En general, esta representación simétrica de $\mathbb{Z}_m$ es $\{-\lfloor (m-1)/2 \rfloor, \ldots, \lfloor m/2 \rfloor\}$, si bien se toma el representante positivo con valor $n/2$ cuando n es par, por ejemplo, $\mathbb{Z}_{10} = \{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$.

Actividad 18.13

Son las 17 horas, quedamos dentro de 82 horas, ¿cuándo es esto?

[Cubit 111].

Ejemplo 539

Debemos elegir entre cinco objetos a, b, c, d y e, y decidimos hacerlo poniendo los objetos en una fila, numerándolos de 1 a 5 y contando hasta un número grande. Comenzando a contar, 1, 2, 3, 4, 5 y así, llegado el último, seguir en el penúltimo que sería 6 y hacia atrás, hasta el primero que sería 9, etc., de esta forma:

$$\begin{array}{cccccc c} & a & b & c & d & e & \\ \hline & 1 & 2 & 3 & 4 & 5 & \\ & 9 & 8 & 7 & 6 & 5 & \hookleftarrow \\ \hookrightarrow & 9 & 10 & 11 & 12 & 13 & \\ & 17 & 16 & 15 & 14 & 13 & \hookleftarrow \\ \hookrightarrow & 17 & 18 & 19 & 20 & 21 & \ldots \end{array} \tag{18.4}$$

entonces, si hemos decidido parar cuando lleguemos a 1234, ¿en qué objeto acaba la cuenta?

[Cubit 112].

Resolución.— Si queremos resolver esta cuestión usando un modelo de reloj de n horas, ¿cuántas horas tendría el reloj? ¿Usamos módulo 5? Para 15 (en vez de 1234) no sirve el módulo 5.

Pensemos en las clases de restos, $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$, entonces $[m] = [0]$, $[m+1] = [1]$, y así sucesivamente. Buscamos la primera coincidencia de $[1]$ con otra clase. Resulta que la primera coincidencia de $[1]$ con otra clase es con la clase $[9]$. De aquí que el módulo sea 8.

Se trata de un reloj de 8 horas. Puede que nos confunda el hecho de haber empezado la cuenta en 1 en vez de en 0 pero quedémonos con que la primera coincidencia con $[1]$ la tiene $[9]$ por lo que el módulo es 8. En definitiva, es un reloj de 8 horas y, entonces, $1234 \bmod 8 = 2$, así que nuestras amistades elegirán el tercer regalo.

Puede que se vea mejor analizando las columnas que reflejan la manera de contar. Observemos que, en realidad, en las columnas de la matriz 18.4 están los restos implícitos, por ejemplo, en la primera, 1, 9 y 17 todos dan resto 1 al dividir entre 8, en la segunda identificamos dos tipos, los que dan resto 2 y los que dan resto 0, y así sucesivamente

- columna r_1 es $[1]_{(8)} = \{1, 9, 17, \ldots\}$,

- columna r_2 es $[2]_{(8)} \cup [0]_{(8)} = \{2, 10, 18, \ldots\} \cup \{8, 16, 24, \ldots\}$,
- columna r_3 es $[3]_{(8)} \cup [7]_{(8)} = \{3, 11, 19, \ldots\} \cup \{7, 15, 23, \ldots\}$,
- columna r_4 es $[4]_{(8)} \cup [6]_{(8)} = \{4, 12, 20, \ldots\} \cup \{6, 14, 22, \ldots\}$,
- columna r_5 es $[5]_{(8)} = \{5, 13, 21, \ldots\}$. ■

Teorema 18.68 (Propiedades generales, I)

$\forall a, b, c, d, k, r \in \mathbb{Z}, \forall d, m, n \in \mathbb{Z}^+, \forall n \in \mathbb{N}$:

0. $a \equiv b \pmod{1}$;
1. si D mód $d = r$ y $0 \leq r < |d|$, entonces $D \equiv r \pmod{d}$;
2. siendo $a \equiv b \pmod{m}$, si $d \mid m$, entonces $a \equiv b \pmod{d}$;
3. si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces:
   0. $a + c \equiv b + d \pmod{m}$, (aditiva)
   1. $ka \equiv kb \pmod{m}$; (producto por escalar entero)
   2. $ka + rc \equiv kb + rd \pmod{m}$; (linealidad entera)
   3. $ac \equiv bd \pmod{m}$, (multiplicativa)
4. si $a \equiv b \pmod{m}$, entonces $a^n \equiv b^n \pmod{m}$; (potencia)
5. si $a \equiv b \pmod{m}$, entonces $f(a) \equiv f(b) \pmod{m}$, para cualquier polinomio f con coeficientes enteros. (polinómica)

Observación 18.5.1.— La propiedad producto por un escalar entero es un caso particular de la propiedad polinómica, siendo f el polinomio $f(x) = kx$.

Ejemplo 540

Demostremos que $\forall n \in \mathbb{N}, 23^n + 1$ es par.

[EFE Coincidencias 25.1.2019:4].

Resolución.— Debemos demostrar que $\forall n \in \mathbb{N}, 23^n + 1 \equiv 0 \pmod{2}$. En efecto:

$$\begin{aligned}
&23 \equiv 1 \pmod{2} && \\
\rightarrow\ &23^n \equiv 1^n = 1 \pmod{2} && \text{[potencia]} \\
\leftrightarrow\ &23^n \equiv -1 \pmod{2} && \text{[transitiva con } 1 \equiv -1 \pmod{2}\text{]} \\
\rightarrow\ &23^n + 1 \equiv 0 \pmod{2}, && \text{[aditiva con } 1 \equiv 1 \pmod{2}\text{]}
\end{aligned}$$

lo cual equivale, por definición de congruencia, a que $23^n + 1$ es múltiplo de 2, en otras palabras, par. ■

Ejemplo 541

En el mismo supuesto del ejemplo 539 (pág. 991 de esta edición), pero ahora imaginemos que tuviésemos que contar hasta un número enorme, por ejemplo, 12 345 678 912 345 678. ¿Cómo pudiésemos hacer esto y cuál sería el objeto elegido?

[Cubit 113].

Resolución.— Observemos que $12\,345\,678\,912\,345\,678 = 12\,345\,678\,912\,345 \cdot 10^3 + 678$. Por un lado, como $10^3 \equiv 0 \pmod{8}$, esto es, $10^3 \bmod 8 = 0 \bmod 8$, entonces $12\,345\,678\,912\,345 \cdot 10^3 \equiv 0 \pmod{8}$. Por otro, $678 \equiv 6 \pmod{8}$. Ahora, por la propiedad aditiva (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) de las congruencias, es admisible sumar miembro a miembro estas dos:

$$12\,345\,678\,912\,345 \cdot 10^3 + 678 \equiv 0 + 6 \pmod{8},$$

por tanto, $12\,345\,678\,912\,345\,678 \equiv 6 \pmod{8}$.

Solución.— Ya hemos visto cómo hacerlo; el objeto elegido es d, el cuarto. ■

Ejemplo 542

En el sistema de numeración decimal (base 10), demostremos que si n es un número natural, entonces el resto de dividir 2^{3n} por 7 es 1.

[EFE 7.7.2021:5a]. *Cfr.* García, Hernández y Nevot [150]: problema propuesto (y resuelto) 1.19 (págs. 41 y 53).

Resolución.— En efecto, como el resto de dividir $2^3 = 8$ entre 7 es 1, entonces, multiplicando sucesivamente congruencias miembro a miembro (propiedad multiplicativa —*vid. supra* teorema 18.68 [pág. 992 de esta edición]—):

$$\begin{aligned} 2^3 &\equiv 1 \pmod{7} \\ \to 2^3 \cdot 2^3 \equiv 1 \cdot 1 \pmod{7} \to 2^{3\cdot 2} &\equiv 1 \pmod{7} \\ \to 2^3 \cdot 2^{3\cdot 2} \equiv 1 \cdot 1 \pmod{7} \to 2^{3\cdot 3} &\equiv 1 \pmod{7} \\ &\vdots \\ \to 2^3 \cdot 2^{3\cdot(n-1)} \equiv 1 \cdot 1 \pmod{7} \to 2^{3\cdot n} &\equiv 1 \pmod{7}, \end{aligned}$$

lo cual equivale, por definición de congruencia, a que el resto de dividir 2^{3n} por 7 es 1. ■

Observación 18.5.2.— Alternativamente, más breve, utilizando la propiedad de potencia siendo $n \in \mathbb{N}$:

$$2^3 \equiv 1 \pmod 7$$
$$\to (2^3)^n \equiv 1^n = 1 \pmod 7.$$

Ejemplo 543

En el sistema decimal, al dividir entre 4 el divisor d, el cociente entero q y el resto r de una división, se obtienen los restos 1, 2 y 3, respectivamente. ¿Cuál es el dividendo D de dicha división si se sabe que D es el mayor número de 3 cifras decimales que satisface lo dicho?

[EFO 3.6.2019:4a]. *Cfr.* Anzola y Caruncho [197]: problema 9.14 (pág. 212).

Resolución.— Según el enunciado:

$$d \equiv 1 \pmod 4, \tag{18.5}$$
$$q \equiv 2 \pmod 4, \tag{18.6}$$
$$r \equiv 3 \pmod 4, \tag{18.7}$$

Como por el algoritmo de Euclides, $D = dq + r$, entonces, por las propiedades multiplicativa y aditiva de las congruencias (*vid. supra* teorema 18.68 [pág. 992 de esta edición]),

$$\begin{aligned} D &\equiv 1 \cdot 2 + 3 \pmod 4 \\ &\equiv 5 \pmod 4 \\ &\equiv 1 \pmod 4, \end{aligned} \tag{18.8}$$

de donde se sigue que $(D - 1)$ es divisible por 4.

Por otro lado, el mayor número de 3 cifras divisible por 4 es 996, por lo que $D - 1 = 996$.

Solución.— El valor del dividendo D es 997. ■

Ejemplo 544

Demostremos que $n(n^2 + 5)$ es divisible por 6 para todo $n \in \mathbb{N}$.

[EFO 3.6.2019:4b]. *Cfr.* Anzola y Caruncho [197]: problema 7.89 (pág. 174).

Resolución.— Como la diferencia entre los números $(n^2 + 5)$ y $(n^2 - 1)$ es 6, ambos son congruentes módulo 6, de donde, por la propiedad multiplicativa de las congruencias (*vid. supra* teore-

ma 18.68 [pág. 992 de esta edición]), multiplicando lado a lado la congruencia

$$n^2 + 5 \equiv n^2 - 1 \pmod{6}$$

por la congruencia

$$n \equiv n \pmod{6},$$

se tiene que

$$\begin{aligned} n(n^2+5) &\equiv n(n^2-1) \pmod{6} \\ &\equiv n(n-1)(n+1) \pmod{6} \\ &\equiv 0 \pmod{6}, \end{aligned}$$

ya que se trata del producto de tres números consecutivos $(n-1)n(n+1)$, de donde uno debe ser múltiplo de 2 (pues al dividir entre 2 sólo hay dos restos posibles) y otro de 3 (ya que al dividir por 3 sólo hay tres restos posibles) y, por tanto, dicho producto ha de ser múltiplo de 6. ■

Ejemplo 545

Dados $a, b, c \in \mathbb{Z}^+$, calculemos el resto de dividir s entre a utilizando el algoritmo de la división o la teoría de congruencias (el «o» es inclusivo), sabiendo que $a \mid b$ y que el resto de dividir c entre a es r y que el resto de dividir c entre b es s.

[AIC 10.4.2019:5a].

Resolución.— Sabemos que

$$b \equiv 0 \pmod{a}, \tag{18.9}$$

$$c \equiv r \pmod{a}, \tag{18.10}$$

y que

$$c \equiv s \pmod{b}; \tag{18.11}$$

además, de esta última, por el algoritmo de la división (*vid. supra* teorema 18.8 [pág. 949 de esta edición]), se sigue que

$$\exists! q \in \mathbb{Z}, c = qb + s, \tag{18.12}$$

pudiéndose reescribir entonces la congruencia (18.10) como

$$qb + s \equiv r \pmod{a}. \tag{18.13}$$

Por otro lado, de la congruencia (18.9), por la propiedad producto por un escalar entero (*vid. supra* teorema 18.68 [pág. 992 de esta edición]), se sigue que

$$-qb \equiv 0 \pmod{a}. \tag{18.14}$$

Finalmente, por la propiedad aditiva (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) de las congruencias, sumando (18.14) de (18.13), miembro a miembro, obtenemos que

$$s \equiv r \pmod{a},$$

en otras palabras, el resto de dividir s por a es r. ■

Ejemplo 546

Utilizando el algoritmo de la división o la teoría de congruencias (el «o» es inclusivo), demostremos que $7^n(3n-7)+7$ es divisible por 3 para todo $n \in \mathbb{N}$.

[AIC 10.4.2019:5b]. *Cfr.* Anzola y Caruncho [197]: problema 7.30 (pág. 150).

Resolución.— Como sea cual sea $n \in \mathbb{N}$, $3n$ es múltiplo de 3, esto es:

$$3n \equiv 0 \pmod{3},$$

entonces, por la propiedad aditiva (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) de las congruencias, sumando miembro a miembro la anterior con

$$-7 \equiv -7 \pmod{3},$$

se tiene que

$$3n-7 \equiv -7 \pmod{3},$$

y como

$$7 \equiv 1 \pmod{3},$$

y por la propiedad potencia (*vid. supra* teorema 18.68 [pág. 992 de esta edición]),

$$7^n \equiv 1^n = 1 \pmod{3},$$

entonces, por la propiedad multiplicativa (*vid. supra* teorema 18.68 [pág. 992 de esta edición]), multiplicándolas lado a lado,

$$7^n(3n-7) \equiv 1 \cdot (-7) = -7 \pmod{3},$$

de donde, finalmente, de nuevo por la propiedad aditiva, sumando miembro a miembro,

$$7 \equiv 7 \pmod{3},$$

a la anterior, tenemos que

$$7^n(3n-7)+7 \equiv (-7)+7 = 0 \pmod{3},$$

en otras palabras, $7^n(3n-7)+7$ es divisible por 3 para todo $n \in \mathbb{N}$. ■

Teorema 18.69 (Propiedades generales, II)
$\forall a, b, c \in \mathbb{Z}, \forall d, m \in \mathbb{Z}^+$:

6. cancelación/simplificación de un factor común si el módulo es divisible por dicho factor:
   0. si $a \equiv b \pmod{m}$, entonces $ac \equiv bc \pmod{mc}$; (monotonía)
   1. si $ac \equiv bc \pmod{mc}$ y $c \neq 0$, entonces $a \equiv b \pmod{m}$; (cancelación)
7. si $ac \equiv bc \pmod{m}$ y $d = \text{mcd}(c, m)$, entonces $a \equiv b \pmod{m/d}$; (simplificación)
8. si $ac \equiv bc \pmod{m}$ y m es primo y $m \nmid c$, entonces $a \equiv b \pmod{m}$. (simplificación primal)

Teorema 18.70 (Propiedades generales, III)
$\forall a, b \in \mathbb{Z}, \forall d, m, n \in \mathbb{Z}^+$:

9. siendo $a \equiv b \pmod{m}$, si $d \mid a$ y $d \mid m$, entonces $d \mid b$;
10. si $a \equiv b \pmod{m}$, entonces $\text{mcd}(a, m) = \text{mcd}(b, m)$;
11. si $a \equiv b \pmod{m}$ y $0 \leq |b - a| < m$, entonces, $a = b$;
12. $a \equiv b \pmod{m}$ si, y sólo si, $a \bmod m = b \bmod m$;
13. si $a \equiv b \pmod{m}$, $a \equiv b \pmod{n}$ y $\text{mcd}(m, n) = 1$, entonces $a \equiv b \pmod{mn}$;

Actividad 18.14

Encontremos información sobre el *algoritmo de* LUHN de validación de ciertos números de identificación y entendamos su funcionamiento.*

* Un punto de partida: https://es.wikipedia.org/wiki/Algoritmo_de_Luhn.

§ 18.6 Aritmética modular

En $\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$, se definen la *suma* y el *producto*; hablamos de *aritmética en* $\mathbb{Z}_m$ o, sinónimamente, de *aritmética módulo* m.

Observación 18.6.0.— La notación se relaja frecuentemente. Los elementos de $\mathbb{Z}_m$, si queremos destacar que son clases de equivalencia se notan $[x]_{(m)}$, $[x]_m$, $\bar{x}_{(m)}$, $\bar{x}_m$ o $[x]$ o $\bar{x}$ si está claro el módulo. Pero también suelen notarse simplemente x. En analogía, las operaciones pueden notarse con subíndices $+_{(m)}, -_{(m)}, \cdot_{(m)}, +_m, -_m, \cdot_m$ o sin ellos, $+, -, \cdot$, siempre que sepamos en qué $\mathbb{Z}_m$ trabajamos.

Observación 18.6.1.— Notemos que la aritmética módulo m traza una correspondencia de todos los enteros $\mathbb{Z}$ al conjunto $\mathbb{Z}_m$.

Observación 18.6.2.— Los resultados de las operaciones son independientes de los representantes elegidos de las clases de equivalencia.

§ 18.6.0 Suma modular

Definición 18.25.— $\forall [a]_m, [b]_m \in \mathbb{Z}_m$,

$$[a]_m + [b]_m = [a+b]_m = \{n \in \mathbb{Z} : n \equiv a+b \pmod{m}\},$$

es decir,

$$((a \bmod m) + (b \bmod m)) \bmod m = (a+b) \bmod m.$$

Observación 18.6.3.— También se define la diferencia; $\forall [a]_m, [b]_m \in \mathbb{Z}_m$,

$$[a]_m - [b]_m = [a-b]_m = \{n \in \mathbb{Z} : n \equiv a-b \pmod{m}\},$$

es decir,

$$((a \bmod n) - (b \bmod n)) \bmod n = (a-b) \bmod n.$$

Ejemplo 547

Hallemos $2+3$ y $2-3$ en $\mathbb{Z}_5$.

Resolución.— $2+3=0$ y $2-3=4$ en $\mathbb{Z}_5$, ya que $2+3 \equiv 0 \pmod{5}$ y $2-3 \equiv 4 \pmod{5}$. ■

Ejemplo 548

¿Cuál es la tabla de Cayley de $+_5$, es decir, de la suma en $\mathbb{Z}_5$?

Resolución.— La tabla de Cayley de $+_5$, la suma en $\mathbb{Z}_5$, es la siguiente. Recordemos que $\forall a, b, c \in \mathbb{Z}_5$,

$$a +_5 b = c \leftrightharpoons a+b \equiv c \pmod{5}.$$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

■

Actividad 18.15

Observemos esta última tabla: la antidiagonal, todos 4; sus paralelas, hacia el noroeste, 3,

2, 1 y 0, y hacia el sureste, 0, 1, 2. ¿Alguna explicación? (Porque desde luego, así se recuerda bien la tabla).

Teorema 18.71 (Estructura algebraica de $\langle \mathbb{Z}_m; +\rangle$)
$\langle \mathbb{Z}_m; +\rangle$ *es un grupo abeliano*, esto es, se satisfacen las propiedades:

0. *conmutativa*: $\forall a, b \in \mathbb{Z}_m$ $(a+b)$ mód $m = (b+a)$ mód m, esto es, $a + b \equiv b + a \pmod{m}$;
1. *asociativa*: $\forall a, b, c \in \mathbb{Z}_m$, $((a+b)+c)$ mód $m = (a+(b+c))$ mód m, esto es, $(a+b)+c \equiv a+(b+c) \pmod{m}$;
2. *elemento neutro*: $\exists 0 \in \mathbb{Z}_m$, $\forall a \in \mathbb{Z}_m$, a mód $m = (0+a)$ mód $m = (a+0)$ mód m, esto es, $a \equiv 0 + a \equiv a + 0 \pmod{m}$;
3. *elemento simétrico*: $\forall a \in \mathbb{Z}_m$, $\exists a' \in \mathbb{Z}_m$, tal que 0 mód $m = (a'+a)$ mód $m = (a+a')$ mód m, esto es, tal que $0 \equiv a' + a \equiv a + a' \pmod{m}$.

§ 18.6.1 Producto modular

Definición 18.26.— $\forall [a]_m, [b]_m \in \mathbb{Z}_m$,

$$[a]_m \cdot [b]_m = [ab]_m = \{n \in \mathbb{Z} : n \equiv ab \pmod{m}\},$$

es decir,

$$((a \text{ mód } n) \cdot (b \text{ mód } n)) \text{ mód } n = (a \cdot b) \text{ mód } n.$$

Ejemplo 549

Hallemos $2 \cdot 3$ en $\mathbb{Z}_5$.

Resolución.— $2 \cdot 3 = 1$ en $\mathbb{Z}_5$, ya que $(2 \cdot 3)$ mód $5 = 1$, es decir, $2 \cdot 3 \equiv 1 \pmod{5}$. ■

Ejemplo 550

¿Cuál es la tabla de Cayley de $\cdot_5$, es decir, del producto en $\mathbb{Z}_5$?

Resolución.— La tabla de Cayley de $\cdot_5$, el producto en $\mathbb{Z}_5$, es la siguiente. Recordemos que $\forall a, b, c \in \mathbb{Z}_5$,

$$a \cdot_5 b = c \leftrightharpoons a \cdot b \equiv c \pmod{5}.$$

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

■

Teorema 18.72 (Estructura algebraica de $\langle \mathbb{Z}_m; \cdot \rangle$)
$\langle \mathbb{Z}_m; \cdot \rangle$ *es un monoide abeliano*, esto es, se satisfacen las propiedades:

0. *conmutativa*: $\forall a, b \in \mathbb{Z}_m$, $(a \cdot b) \text{ mód } m = (b \cdot a) \text{ mód } m$, esto es, $a \cdot b \equiv b \cdot a \pmod{m}$;
1. *asociativa*: $\forall a, b, c \in \mathbb{Z}_m$, $((a \cdot b) \cdot c) \text{ mód } m = (a \cdot (b \cdot c)) \text{ mód } m$, esto es, $(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{m}$;
2. *elemento neutro*: $\exists 0 \in \mathbb{Z}_m$, $\forall a \in \mathbb{Z}_m$, $a \text{ mód } m = (1 \cdot a) \text{ mód } m = (a \cdot 1) \text{ mód } m$, esto es, $a \equiv 1 \cdot a \equiv a \cdot 1 \pmod{m}$.

§ 18.6.2 De los simétricos aditivos y multiplicativos

Recordemos sus definiciones, dado $a \in \mathbb{Z}_m$:

- $-a$ es el simétrico aditivo de a en $\langle \mathbb{Z}_m; + \rangle$ si, y sólo si, $a + (-a) \equiv 0 \pmod{m}$, y
- a^{-1} es el simétrico multiplicativo de a en $\langle \mathbb{Z}_m; \cdot \rangle$ si, y sólo si, $a \cdot a^{-1} \equiv 1 \pmod{m}$.

Ejemplo 551

¿Qué hay de los simétricos aditivos y multiplicativos en $\mathbb{Z}_5$?

Resolución.— En $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, comprobamos:

- en la tabla de Cayley de la adición que $-0 = 0$, $-1 = 4$, $-2 = 3$, $-3 = 2$ y $-4 = 1$ ($-a$ es la notación habitual para el opuesto [el simétrico aditivo] de un elemento);
- en la tabla de Cayley de la multiplicación que $\nexists 0^{-1}$, $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$ y $4^{-1} = 4$ (a^{-1} es la notación habitual para el recíproco [el simétrico multiplicativo] de un elemento). ■

Insistamos en lo que ha sucedido en el caso multiplicativo —recordemos una vez más la definición: $a \cdot a^{-1} \equiv 1 \pmod{m}$ (al ser $\cdot$ conmutativa, $a \cdot a^{-1} = a^{-1} \cdot a$)—. Todo elemento de $\mathbb{Z}_5$ tiene simétrico aditivo y todo elemento no nulo de $\mathbb{Z}_5$ tiene simétrico multiplicativo. Así es, en general, no existe un simétrico multiplicativo para todo elemento no nulo de $\mathbb{Z}_m$, esto es, para un m arbitrario, no es verdad que para cada $a \in \mathbb{Z}_m$, no nulo, exista un $a^{-1} \in \mathbb{Z}_m$ tal que $a \cdot a^{-1} \equiv 1 \pmod{m}$.

Ejemplo 552

Calculemos en $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ los simétricos aditivos de cada elemento de $\mathbb{Z}_8$ y los multiplicativos de los elementos no nulos, siempre que sea posible.

Observación.— Pudiésemos construir las tablas de CAYLEY o aplicar directamente las definiciones de simétrico aditivo y simétrico multiplicativo; a nuestra elección.

Resolución.— Veamos:

- es cierto que en $\mathbb{Z}_8$ todo elemento a tiene un simétrico aditivo $-a$: $-0 = 0$, $-1 = 7$, $-2 = 6$, $-3 = 5$, $-4 = 4$, $-5 = 3$, $-6 = 2$, $-7 = 1$; esto es así por definición de simétrico aditivo $a + a' \equiv 0 \pmod{m}$, por ejemplo, como $(2 + 6) \bmod 8 = 0 \bmod 8$, el simétrico aditivo de 2 es 6; por cierto, fijémonos también en la notación para los simétricos aditivos —los opuestos—, $-a$;
- pero no todo elemento no nulo a de $\mathbb{Z}_8$ tiene un simétrico multiplicativo a^{-1}: $\nexists 0^{-1}$, $1^{-1} = 1$, $\nexists 2^{-1}$, $3^{-1} = 3$, $\nexists 4^{-1}$, $5^{-1} = 5$, $\nexists 6^{-1}$, $7^{-1} = 7$; esto es así por definición de simétrico multiplicativo $a \cdot a^{-1} \equiv 1 \pmod{m}$, por ejemplo, como $(5 \cdot 5) \bmod 8 = 1 \bmod 8$, el simétrico multiplicativo de 5 es 5; por cierto, fijémenos también en la notación para los simétricos multiplicativos —los recíprocos—, a^{-1}. ■

Observemos que los simétricos multiplicativos sólo existen para aquellos elementos de $\mathbb{Z}_8$ que son coprimos con 8.

Y esto es un teorema.

Teorema 18.73
Los simétricos multiplicativos —esto es, las soluciones de $ax \equiv 1 \pmod{m}$— existen sólo para aquellos elementos de $a \in \mathbb{Z}_m$ que son coprimos con m.

Demostración.— Esto es así porque mientras que la siguiente propiedad de simplificación de la adición módulo m,

$$\text{si } (a + b) \equiv (a + c) \pmod{m}, \text{ entonces } b \equiv c \pmod{m},$$

es la misma que para la adición ordinaria, la multiplicación módulo m no satisface una propiedad similar, esto es,

$$(a \cdot b) \equiv (a \cdot c) \pmod{m} \text{ no implica } b \equiv c \pmod{m},$$

a menos que a y m sean primos entre sí. ■

Notemos por $\mathbb{Z}_m^\times$ el conjunto de los elementos multiplicativamente simetrizables de $\mathbb{Z}_m$, si bien en la literatura figura también la designación $\mathbb{Z}_m^*$ (que en tales textos no debemos confundir con $\mathbb{Z}_m \setminus \{0\}$).

Observación 18.6.4.— Notando $t(m) = \{k \in \mathbb{Z}^+ : 1 \leq k < m, \operatorname{mcd}(k, m) = 1\}$, lo establecido por el teorema 18.73 (pág. 1001 de esta edición) es que $\mathbb{Z}_m^\times = t(m)$.

Teorema 18.74 (Estructura algebraica de $\langle \mathbb{Z}_m^\times; \cdot \rangle$)
$\langle \mathbb{Z}_m^\times; \cdot \rangle$ es un grupo abeliano, el *grupo abeliano multiplicativo de las unidades de* $\mathbb{Z}_m$.

Teorema 18.75 (Cardinalidad de $\mathbb{Z}_m^\times$)
El cardinal de $\mathbb{Z}_m^\times$ es $\varphi(m)$.

Ejemplo 553

Comprobemos que $|\mathbb{Z}_5^\times| = \varphi(5)$.

Resolución.— En efecto, como apreciamos en la resolución del ejemplo 550 (pág. 999 de esta edición), en la tabla de Cayley, $\nexists 0^{-1}, 1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2$ y $4^{-1} = 4$; luego, $\mathbb{Z}_5^\times = \{1, 2, 3, 4\}$, cuyo cardinal es 4, justamente el valor de $\varphi(5)$ ($5 \in \mathbb{P}$, y sabemos que si p es primo, $\varphi(p) = p - 1$). ■

Actividad 18.16

Comprobemos que $\varphi(8) = |\mathbb{Z}_8^\times|$.

§ 18.6.3 El anillo $\mathbb{Z}/m\mathbb{Z}$ de los enteros módulo m

Teorema 18.76
En $\langle \mathbb{Z}_m; +, \cdot \rangle$ se satisface que $\cdot$ es distributiva respecto de $+$, esto es, $\forall a, b, c \in \mathbb{Z}_m$, $(a \cdot (b + c)) \text{ mód } m = ((a \cdot b) + (a \cdot c)) \text{ mód } m$, es decir, $a(b + c) \equiv ab + ac \pmod{m}$.

Teorema 18.77
$\langle \mathbb{Z}_m; +, \cdot \rangle$ es un *anillo abeliano unitario*, que suele notarse $\mathbb{Z}/m\mathbb{Z}$, o, sinónimamente, $\mathbb{Z}/(m)$.

Demostración.— Por ser $\langle \mathbb{Z}_m; + \rangle$ grupo abeliano y $\langle \mathbb{Z}_m; \cdot \rangle$ monoide abeliano y ser $\cdot$ distributiva respecto de $+$. ■

Observación 18.6.5.— Se tiene el homomorfismo de anillos $h_m : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$, definido por $h_m(x) = [x]_m$ tal que

$$h_m(x+y) = h_m(x) +_m h_m(y),$$
$$h_m(x \cdot y) = h_m(x) \cdot_m h_m(y).$$

Observación 18.6.6.— Alternativamente, como sucede en algunos textos, pudiésemos notar $\mathbb{Z}/m^{\times}$ por $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

Teorema 18.78

$\mathbb{Z}/m\mathbb{Z}$ no es un dominio de integridad.

Demostración.— No es un dominio de integridad, pues, aunque $\mathbb{Z}/m\mathbb{Z}$ posee elemento neutro para la multiplicación, no satisface la definición de dominio de integridad que exige la no existencia de divisores de cero, esto es, que si $a \cdot b = 0$ entonces o a o b deben ser cero; de hecho, existen divisores de cero en $\mathbb{Z}/m\mathbb{Z}$ si m no es primo; por ejemplo, como $2 \cdot 3 \equiv 0 \pmod 6$, 2 y 3 son divisores de cero en $\mathbb{Z}/6\mathbb{Z}$. ■

Actividad 18.17

Demostremos que $\mathbb{Z}/m\mathbb{Z}$ tampoco tiene estructura de cuerpo.

§ 18.6.4 Estructuras algebraicas con módulo primo

Teorema 18.79

Si p es primo, $\langle \mathbb{Z}_p; \cdot \rangle$ es un grupo abeliano.

Teorema 18.80

Si p es primo, $\langle \mathbb{Z}_p; \cdot \rangle$ es un grupo cíclico, esto es, existe al menos un elemento que es capaz de generar a todos los demás.

Ejemplo 554

Demostremos que 3 es un generador de $\langle \mathbb{Z}_7; \cdot \rangle$.

Resolución.— En efecto, se satisface: $3^1 \equiv 3 \pmod 7$, $3^2 = 9 \equiv 2 \pmod 7$, $3^3 = 27 \equiv 6 \pmod 7$, $3^4 = 81 \equiv 4 \pmod 7$, $3^5 = 243 \equiv 5 \pmod 7$, $3^6 = 729 \equiv 1 \pmod 7$ (como $3^6 \equiv 1 \pmod 7$, entonces $3^7 \equiv 3 \pmod 7$, es decir, las potencias entran en un ciclo); abreviadamente, notamos $\langle \mathbb{Z}_7; \cdot \rangle = < 3 >$. ■

Teorema 18.81

Si p es primo, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo finito, a veces llamado *cuerpo finito primo*.

Demostración.— Observemos que todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ será coprimo con p ('no nulo' significa distinto del elemento neutro de la operación aditiva) y eso implica que existirá en $\mathbb{Z}/p\mathbb{Z}$ un simétrico multiplicativo para todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$, por tanto, $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo finito. ■

Actividad 18.18

Como complemento al teorema 18.81 (pág. 1004 de esta edición), demostremos que si p es primo, todo elemento no nulo de $\mathbb{Z}/p\mathbb{Z}$ posee un único simétrico multiplicativo en $\mathbb{Z}/p\mathbb{Z}$.
Sugerencia.— Intentémoslo por reducción al absurdo.

Observación 18.6.7.— Si p es primo, $\mathbb{Z}_p^\times$ coincide con $\mathbb{Z}_p$ por lo que todo lo dicho para éste es válido para aquél.

§ 18.6.5 Obtención de simétricos multiplicativos

Ejemplo 555

¿Cómo pudiésemos encontrar simétricos multiplicativos en $\mathbb{Z}/m\mathbb{Z}$ usando la identidad de BÉZOUT?

Resolución.— Recordemos la definición de simétrico multiplicativo de a, a saber, $a \cdot a^{-1} \equiv 1 \pmod{m}$.

Por la discusión hecha hasta ahora, existen los simétricos multiplicativos para todo $a \in \mathbb{Z}_m$ tales que a es coprimo con m, esto es, $\operatorname{mcd}(a, m) = 1$—si m es igual a un primo p, esto lo satisfarán siempre todos los elementos no nulos—.

De acuerdo con la identidad de BÉZOUT, para algunos enteros s y t—que pueden ser positivos o negativos o cero— se satisface: $s \cdot a + t \cdot m = 1$.

Observemos que como t es entero, $t \cdot m \equiv 0 \pmod{m}$, entonces, debe suceder que $s \cdot a \equiv 1 \pmod{m}$, por tanto s, el primer coeficiente de BÉZOUT, es el simétrico multiplicativo módulo m de a—recordemos que $\cdot$ es conmutativa, $s \cdot a = a \cdot s$—. En consecuencia, cualquier algoritmo para calcular s para a, m, siendo $\operatorname{mcd}(a, m) = 1$, nos servirá para calcular el simétrico multiplicativo módulo m de a, en particular, el algoritmo de EUCLIDES extendido que ya conocemos. ■

<table>
<tr><th colspan="2">Cuadro resumen de algunas propiedades y peculiaridades de $+$ y $\cdot$ en $\mathbb{Z}_m$</th></tr>
<tr><td>$+$ en $\mathbb{Z}_m$</td><td>$\cdot$ en $\mathbb{Z}_m$</td></tr>
<tr><td colspan="2">$+$ y $\cdot$ son conmutativas en $\mathbb{Z}_m$
$\forall a, b \in \mathbb{Z}_m$</td></tr>
<tr><td>$(a+b) \text{ mód } m = (b+a) \text{ mód } m$
$a + b \equiv b + a \pmod{m}$</td><td>$(a \cdot b) \text{ mód } m = (b \cdot a) \text{ mód } m$
$a \cdot b \equiv b \cdot a \pmod{m}$</td></tr>
<tr><td colspan="2">por lo tanto, $\langle \mathbb{Z}_m; + \rangle$ y $\langle \mathbb{Z}_m; \cdot \rangle$ son magmas abelianos;</td></tr>
<tr><td colspan="2">$+$ y $\cdot$ son asociativas en $\mathbb{Z}_m$
$\forall a, b, c \in \mathbb{Z}_m$</td></tr>
<tr><td>$((a+b)+c) \text{ mód } m = (a+(b+c)) \text{ mód } m$
$(a+b)+c \equiv a+(b+c) \pmod{m}$</td><td>$((a \cdot b) \cdot c) \text{ mód } m = (a \cdot (b \cdot c)) \text{ mód } m$
$(a \cdot b) \cdot c \equiv a \cdot (b \cdot c) \pmod{m}$</td></tr>
<tr><td colspan="2">por lo tanto, $\langle \mathbb{Z}_m; + \rangle$ y $\langle \mathbb{Z}_m; \cdot \rangle$ son semigrupos abelianos;</td></tr>
<tr><td colspan="2">existen elementos neutros para $+$ y $\cdot$ en $\mathbb{Z}_m$
$\exists\, 0, 1 \in \mathbb{Z}_m, \forall a \in \mathbb{Z}_m,$</td></tr>
<tr><td>$a \text{ mód } m = (0 + a) \text{ mód } m = (a + 0) \text{ mód } m$
$a \equiv 0 + a \equiv a + 0 \pmod{m}$</td><td>$a \text{ mód } m = (1 \cdot a) \text{ mód } m = (a \cdot 1) \text{ mód } m$
$a \equiv 1 \cdot a \equiv a \cdot 1 \pmod{m}$</td></tr>
<tr><td colspan="2">por lo tanto, $\langle \mathbb{Z}_m; + \rangle$ y $\langle \mathbb{Z}_m; \cdot \rangle$ son monoides abelianos;</td></tr>
<tr><td colspan="2">acerca de los simétricos aditivos y multiplicativos</td></tr>
<tr><td>todo elemento de $\mathbb{Z}_m$ tiene un simétrico aditivo
$\forall a \in \mathbb{Z}_m, \exists a' \in \mathbb{Z}_m,$
$0 \text{ mód } m = (a' + a) \text{ mód } m = (a + a') \text{ mód } m$
$0 \equiv a' + a \equiv a + a' \pmod{m}$</td><td>existen elementos de $\mathbb{Z}_m$ sin simétrico multiplicativo
$\exists a \in \mathbb{Z}_m, \nexists a' \in \mathbb{Z}_m,$
$1 \text{ mód } m = (a' \cdot a) \text{ mód } m = (a \cdot a') \text{ mód } m$
$1 \equiv a' \cdot a \equiv a \cdot a' \pmod{m}$</td></tr>
<tr><td colspan="2">por lo tanto, $\langle \mathbb{Z}_m; + \rangle$ es grupo abeliano
y $\langle \mathbb{Z}_m; \cdot \rangle$ no es grupo;</td></tr>
<tr><td colspan="2">$\cdot$ es distributiva respecto de $+$
$\forall a, b, c \in \mathbb{Z}_m$
$(a \cdot (b + c)) \text{ mód } m = ((a \cdot b) + (a \cdot c)) \text{ mód } m$
$a(b+c) \equiv ab + ac \pmod{m}$</td></tr>
<tr><td colspan="2">por lo tanto, $\langle \mathbb{Z}_m; +, \cdot \rangle$, esto es, $\mathbb{Z}/m\mathbb{Z}$, es anillo abeliano unitario;</td></tr>
<tr><td colspan="2">además, si p es primo,
$\langle \mathbb{Z}_p; \cdot \rangle$ es grupo cíclico
y $\langle \mathbb{Z}_p; +, \cdot \rangle$, esto es, $\mathbb{Z}/p\mathbb{Z}$, es cuerpo.</td></tr>
</table>

§ 18.6.6 Dos pequeñas singularidades

Simulación de valores aleatorios

Es posible generar una secuencia finita de números pseudoaleatorios utilizando aritmética modular —*vid. v. gr.* Revuelta y Ponsoda [206] (págs. 44–45 y págs. 62–64.)—; por ejemplo, el generador de congruencias

$$X_{i+1} = (aX_i + b) \text{ mód } c,$$

con $a, b, c \in \mathbb{Z}^+$, proporciona valores uniformes en el intervalo cerrado $[0, c]$.

Si estuviésemos interesados en simular una secuencia de números pseudoaleatorios en el intervalo cerrado $[0, 1]$, bastaría transformar los anteriores según

$$Y_i = \frac{X_i}{c}.$$

No es difícil demostrar que este generador produce un máximo de c números distintos; de hecho, la secuencia comienza a repetirse tras un número de iteraciones menor o igual que c.

Por ejemplo, para el módulo $c = 7$, el multiplicador $a = 3$, el incremento $b = 1$ y la semilla $X_1 = 1$, el generador produce una secuencia de seis números pseudoaleatorios en el intervalo $[0, 7]$, a saber, 4, 6, 5, 2, 0, 1.

i	X_i	$aX_i + b$	$(aX_i + b)$ mód c
1	1	$3 \cdot 1 + 1 = 4$	4 mód $7 = 4$
2	4	$3 \cdot 4 + 1 = 13$	13 mód $7 = 6$
3	6	$3 \cdot 6 + 1 = 19$	19 mód $7 = 5$
4	5	$3 \cdot 5 + 1 = 16$	16 mód $7 = 2$
5	2	$3 \cdot 2 + 1 = 7$	7 mód $7 = 0$
6	0	$3 \cdot 0 + 1 = 1$	1 mód $7 = 1$
7	1	$3 \cdot 1 + 1 = 4$	4 mód $7 = 4$

Observación 18.6.8.— ¿Por qué números pseudoaleatorios y no aleatorios? Porque son el resultado de una simulación computacional de la aleatoriedad, lo cual supone reglas, por lo que, aparentemente, quien conociese las reglas pudiese conocer el resultado. Pero, ¿y si la computación es cuántica? Pues aún se discute cómo aprovechar la aparente aleatoriedad cuántica a pesar de la aparente no aleatoriedad[31] de los equipamientos y procesos de detección y decisión última actuales. Claro que también pudiese ajustarse el resultado para decrementar su correlación con el

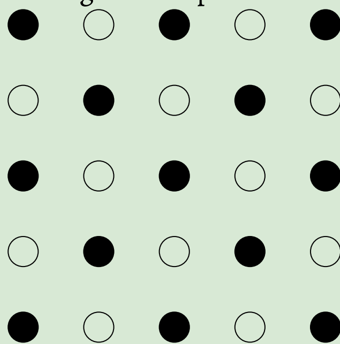
[31] Aparentes por su relatividad desde la realidad de la que quienes observamos formamos parte consciente. ¿Con qué grado de certeza es posible asegurar la no aleatoriedad de lo que consideramos no aleatorio? Igualmente, ¿con qué grado de certeza es posible asegurar la aleatoriedad de lo cuántico? ¿O pudiese ser una co(n)fusión entre grado de existencia, grado de certeza y grado de aleatoriedad?

artefacto que lo proporcionó, lo cual no deja de ser una técnica de doble capa (pudiéndose complicar hasta una de cebolla); asimismo, pudiésemos trabajar con grados de aleatoriedad y, en analogía a lo que actualmente es una regla básica en seguridad informática, procurar que siempre el grado de aleatoriedad de lo «seguro» sea mayor que el grado de aleatoriedad jaqueable.

Lo dicho entronca con el campo del *análisis de seguridad de sistemas*, desde donde el *análisis de fiabilidad* y la *evaluación de riesgos* se complementan para cuantificar razonablemente el comportamiento esperado de un sistema y el riesgo potencial que puede suponer para quienes lo operan, para quienes lo usan y para su entorno, debiéndose desarrollar y establecer un procedimiento de diagnóstico, que busque no sólo identificar las causas más probables de los funcionamientos no correctos, sino que también sirva, vía observaciones y pruebas, para la prevención del deterioro de sus componentes, de la degradación del sistema e, incluso, de la erosión de su obsolescencia, a la vez que se diseñe un plan de acción para la reparación o reemplazo de componentes individuales, de subsistemas o del propio sistema.[32, 33, 34]

Ejemplo 556

¿Qué podrían representar los siguientes puntos?



Resolución.— Pues, por ejemplo, en $\mathbb{Z}_5$, hacemos $(x+y)$ mód 2; así, si es 1, círculo blanco, si no, círculo negro. ■

[32] Este proceso de ayuda a la resolución de problemas es conocido en inglés como *troubleshooting* (*vid. v. gr.* https://en.wikipedia.org/wiki/Troubleshooting) y está emparentado con la *reingeniería de procesos* (*vid. v. gr.* https://en.wikipedia.org/wiki/Business_process_re-engineering).

[33] *Human error, lack of imagination, and blind ignorance. The practice of engineering is in large measure a continuing struggle to avoid making mistakes for these reasons* [El error humano, la falta de imaginación y la ignorancia ciega. La práctica de la ingeniería es, en gran medida, una lucha continua por evitar cometer errores por estas razones]. (Samuel Charles Florman, *The Existential Pleasures of Engineering*, 1976).

[34] Si se utiliza acorde con lo previsto, un diseño de ingeniería no debe fallar; sin embargo, la mayoría de las personas ingenieras desean innovar, lo que les puede llevar a intentar exceder alguna limitación ingenieril; por otra parte, muchos diseños suelen basarse en otros anteriores y pudiese suceder que, presentando fallos estos últimos, no se les preste la atención que merecen, incrementando la probabilidad de que éstos se repitan de insignificante a nada despreciable. A este respecto, merece la pena leer a Henry Petroski, por ejemplo: *To Engineer is Human: The Role of Failure in Successful Design* (1982). Además: «*If something can go wrong, it will* [Si algo puede ir mal, irá]» (ley de Murphy).

§ 18.7 Resolución de congruencias, I

Estudiemos cómo resolver la congruencia lineal $ax \equiv b \pmod{m}$.

Sabemos ya que si $\text{mcd}(a, m) = 1$, es posible expresar la única solución módulo m en función del simétrico multiplicativo de a (que también llamaremos *inverso modular* de a).

Teorema 18.82 (Existencia y unicidad del inverso)
Si $\text{mcd}(a, m) = 1$, la congruencia $ax \equiv 1 \pmod{m}$ tiene una única solución módulo m, a saber, $x \equiv a' \pmod{m}$; llamamos *inverso* de a módulo m a a'.

Ejemplo 557

¿Cuál es el inverso de 7 módulo 23?

a. 7.
b. 8.
c. 9.
d. 10.

[TT], [EFE 3.7.2024:8] (tipo test).

Resolución.—

Vía 0.

Sabemos que $\cdot_{23}$ es conmutativa por lo que basta encontrar un elemento neutro lateral (en la tabla de Cayley de $\cdot_{23}$ vemos que 1 es el neutro por la izquierda) e, igualmente, basta con hallar un simétrico multiplicativo lateral, que en dicha tabla vemos que 10 es el simétrico por la derecha de 7 y, por lo tanto, su inverso único módulo 23.

$\cdot_{23}$	0	$\cdots$	7	8	9	$\boxed{10}$	$\cdots$	22
0	0	$\cdots$	0	0	0	0	$\cdots$	0
1	0	$\cdots$	7	8	9	10	$\cdots$	22
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\boxed{7}$	0	$\cdots$	3	10	17	①	$\cdots$	0
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
22	0	$\cdots$	16	15	14	13	$\cdots$	1

Vía 1.

El inverso de 7 módulo 23 es, caso de existir, la solución única módulo 23 de la ecuación $7x \equiv 1 \pmod{23}$, solución que existe porque $\operatorname{mcd}(7, 23) = 1$ (ya que 23 un número primo).

Utilicemos el algoritmo de Euclides para demostrar que $\operatorname{mcd}(7, 23) = 1$:

$$
\begin{aligned}
23 &= 7 \cdot 3 + 2, \\
7 &= 3 \cdot 2 + 1, \\
2 &= 2 \cdot 1,
\end{aligned}
$$

de donde, como el último resto no nulo es 1, $\operatorname{mcd}(7, 23) = 1$.

Ahora, para encontrar el inverso de 7, recorremos hacia atrás lo anterior (sustitución regresiva con objetivo la identidad de Bézout):

$$
\begin{aligned}
1 &= 7 - 3 \cdot 2, \text{ entonces} \\
1 &= 7 - 3 \cdot (23 - 7 \cdot 3), \text{ de donde} \\
1 &= -3 \cdot 23 + (1 + 3 \cdot 3) \cdot 7, \text{ por lo que} \\
1 &= -3 \cdot 23 + 10 \cdot 7,
\end{aligned}
$$

de donde $-3 \cdot 23 + 10 \cdot 7 \equiv 1 \pmod{23}$ y, como $-3 \cdot 23 \equiv 0 \pmod{23}$, necesariamente $10 \cdot 7 \equiv 1 \pmod{23}$, en otras palabras, 10 es el inverso de 7 módulo 23.

Solución.— Opción d. ■

Observación 18.7.0.— Al ser la del ejemplo anterior una cuestión de opción múltiple con una única respuesta verdadera, probablemente lo más sencillo sea resolverlo por eliminación y comprobación, sustituyendo los valores dados en las opciones, quedando eliminadas las opciones a), b) y c), pues en ellas, respectivamente, $7 \cdot 7 = 49 \equiv 3 \pmod{23}$, $7 \cdot 8 = 56 \equiv 10 \pmod{23}$ y $7 \cdot 9 = 63 \equiv 17 \pmod{23}$; comprobamos que $7 \cdot 10 = 70 \equiv 1 \pmod{23}$.

Actividad 18.19

¿Cuál es el inverso de 3 módulo 13?

a. 3.
b. 6.
c. 9.
d. 12.

[TT], [EFE 29.1.2025:8] (tipo test).

Actividad 18.20

¿Cuál es el inverso de 5 módulo 12?

a. 3.
b. 5.
c. 7.
d. 10.

[TT], [EFEC 29.1.2025:8] (tipo test).

Teorema 18.83 (Existencia y unicidad de la solución)
Si $\operatorname{mcd}(a, m) = 1$, la congruencia lineal $ax \equiv b \pmod{m}$ tiene una única solución módulo m, a saber, $x \equiv ba' \pmod{m}$.

Si $\operatorname{mcd}(a, m) = d$, es posible expresar las d soluciones módulo m en función del inverso modular de a, de m y de d.

Teorema 18.84 (Existencia de solución)
Si d es el $\operatorname{mcd}(a, m)$, la congruencia lineal $ax \equiv b \pmod{m}$ tiene solución si, y sólo si, $d \mid b$. Observemos que si $d \nmid b$, no tiene ninguna solución.

Teorema 18.85 (Existencia, número de soluciones y su cálculo)
Si d es el $\operatorname{mcd}(a, m)$ y $d \mid b$, entonces la congruencia lineal $ax \equiv b \pmod{m}$ tiene d soluciones módulo m que son:

$$\begin{aligned} x &\equiv t + 0 \cdot \frac{m}{d} \pmod{m}, \\ x &\equiv t + 1 \cdot \frac{m}{d} \pmod{m}, \\ x &\equiv t + 2 \cdot \frac{m}{d} \pmod{m}, \\ &\vdots \\ x &\equiv t + (d-1) \cdot \frac{m}{d} \pmod{m}, \end{aligned}$$

donde t es la única solución módulo m/d de la congruencia

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\text{mód}\ \frac{m}{d} \right);$$

solución t que existe y es única [por el teorema 18.82 (pág. 1008 de esta edición), ya que $\operatorname{mcd}(a/d, m/d) = 1$] y que es [por el teorema 18.83 (pág. 1010)]

$$t \equiv \frac{b}{d} \left(\frac{a}{d} \right)' \left(\text{mód}\ \frac{m}{d} \right).$$

Actividad 18.21

Encontremos todas las soluciones módulo 7 de la congruencia lineal $4x \equiv 15 \pmod{7}$, demostrando previamente que tiene solución.

[Cubit 118].

Actividad 18.22

Encontremos todas las soluciones módulo 21 de la congruencia lineal $12x \equiv 45 \pmod{21}$, demostrando previamente que tiene solución.

[Cubit 119].

§ 18.8 Sistemas de residuos

Definición 18.27.— *El menor sistema de residuos* módulo m es el conjunto de enteros $\{0, 1, 2, \ldots, m-1\}$ (no debemos confundirlo con $\mathbb{Z}_m$, el conjunto cociente de $\equiv \pmod{m}$, la relación diádica de equivalencia —aunque por lo general relajemos la notación, debemos saber distinguir cuándo son números y cuándo clases de equivalencia, dependiendo del contexto de trabajo en cada momento—).

Definición 18.28.— Un *sistema completo de residuos* módulo m es cualquier conjunto de m enteros, en el que ningún par de ellos sean congruentes módulo m. Así, un sistema completo de residuos es simplemente un conjunto que contiene precisamente a un representante de cada clase de residuos módulo m.

Observación 18.8.0.— Dadas estas definiciones, se tiene que el menor sistema de residuos módulo m es un sistema completo de residuos módulo m.

Definición 18.29.— Dado un sistema completo de residuos módulo m, un *sistema reducido de residuos* módulo m es el conjunto que queda tras suprimir en él todos los elementos que no son coprimos con m.

Ejemplo 558

Aportemos ejemplos de las definiciones anteriores.

Resolución.— Sean, por ejemplo, los siguientes:

- el menor sistema de residuos módulo 8 es $\{0, 1, 2, 3, 4, 5, 6, 7\}$,
- que además es un sistema completo de residuos módulo 8;
- otro sistema completo de residuos módulo 8 es $\{8, 1, 2, 3, 4, 5, 6, 7\}$ —éste el que usamos en el ejemplo 539 (pág. 991 de esta edición)—;
- otro sistema completo de residuos módulo 8 es $\{-16, -23, 18, 27, -12, 21, -2, -1\}$ —observemos que $-16 \equiv 0 \pmod{8}$, $-23 \equiv 1 \pmod{8}$, $\ldots$, $-1 \equiv 7 \pmod{8}$—;

- un sistema reducido de residuos proveniente del sistema completo anterior es $\{-23, 27, 21, -1\}$;
- otro sistema reducido de residuos módulo 8 es $\{1, 3, 5, 7\}$, que no es otro que $t(8)$, esto es, $\mathbb{Z}_8^\times$ —*cfr. supra* observación 18.6.4 (pág. 1002 de esta edición)—; observemos que proviene de un sistema completo de residuos particular, el menor sistema de residuos módulo 8, esto es, $\mathbb{Z}_8$ visto como conjunto de números. ■

Teorema 18.86 (Cardinalidad)
El cardinal de un sistema reducido de residuos módulo m puede calcularse con la función indicatriz de EULER y es $\varphi(m)$, es decir, $\varphi(m) = |t(m)|$.

Teorema 18.87 (Escalado)
Siendo k entero, si $\{r_0, r_1, \dots, r_n\}$ es un sistema reducido de residuos módulo m y si $\text{mcd}(k, m) = 1$, entonces $\{kr_0, kr_1, \dots, kr_n\}$ es un sistema reducido de residuos módulo m.

§ 18.8.0 Residuos cuadráticos

Definición 18.30.— Siendo $p > 2$ un número primo y $a \in \mathbb{Z}$ tales que $\text{mcd}(a, p) = 1$, decimos que a es un *residuo cuadrático módulo p* precisamente si la ecuación

$$x^2 \equiv a \pmod{p}$$

tiene solución. Si esto no sucede, decimos que a es un *no-residuo cuadrático*.

Teorema 18.88
Hay exactamente $(p-1)/2$ residuos cuadráticos módulo p y $(p-1)/2$ no-residuos cuadráticos módulo p.

Definición 18.31.— Siendo $p > 2$ un número primo y $a \in \mathbb{Z}$ tales que $\text{mcd}(a, p) = 1$, el *símbolo de* LEGENDRE viene definido por

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ es un residuo cuadrático módulo } p \text{ y } a \not\equiv 0 \pmod{p}, \\ -1 & \text{si } a \text{ es un no-residuo cuadrático módulo } p, \\ 0 & \text{si } a \equiv 0 \pmod{p}. \end{cases}$$

Teorema 18.89 (Criterio de EULER)
Siendo $p > 2$ un número primo y $a \in \mathbb{Z}$ tales que $\operatorname{mcd}(a, p) = 1$, se satisface

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Definición 18.32.— Siendo $n \in \mathbb{Z}$ impar, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ su descomposición en factores primos y $a \in \mathbb{Z}$ tales que $\operatorname{mcd}(a, n) = 1$, el *símbolo de* JACOBI viene definido por

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Teorema 18.90 (Los símbolos de LEGENDRE y JACOBI son funciones multiplicativas)
Se satisface:

0. siendo $p > 2$ un número primo y $a, b \in \mathbb{Z}$ tales que $\operatorname{mcd}(ab, p) = 1$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
1. siendo $n \in \mathbb{Z}$ impar y $a, b \in \mathbb{Z}$ tales que $\operatorname{mcd}(ab, n) = 1$, $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

Algoritmos para calcular los símbolos de LEGENDRE y JACOBI

Pudiésemos calcular el símbolo de LEGENDRE mediante el criterio de EULER vía, por ejemplo, el *algoritmo de exponenciación modular*[35]. Para el símbolo de JACOBI, si conocemos la factorización de n, su cálculo se reduce al del símbolo de LEGENDRE, por definición de aquél, si no, y si tuviésemos tiempo e inquietud, pudiese ser recomendable que investigásemos acerca de los diferentes algoritmos para calcularlo.

§ 18.9 El teorema de EULER-FERMAT

Teorema 18.91 (Teorema de EULER-FERMAT)
$(\forall m \in \mathbb{Z}^+)(\forall a \in \mathbb{Z})(\operatorname{mcd}(a, m) = 1 \to a^{\varphi(m)} \equiv 1 \pmod{m})$.

Observación 18.9.0.— En particular, este teorema asegura que

$$(\forall m \in \mathbb{Z}^+)(\forall a \in \mathbb{Z}_m^\times)(a^{\varphi(m)} \equiv 1 \pmod{m}).$$

[35] *Vid. v. gr.* https://en.wikipedia.org/wiki/Modular_exponentiation.

FERMAT lo demostró para m primo —*vid. infra* teorema 18.94 (pág. 1020) (corolario 2.º del teorema de EULER-FERMAT) y el teorema 18.95 (pág. 1021) (teorema pequeño de FERMAT)— y EULER para m entero positivo cualquiera.

Observación 18.9.1.— Pudiésemos ver el teorema de EULER-FERMAT como corolario de ser $\langle \mathbb{Z}_m^\times; \cdot \rangle$ un grupo —*cfr. supra* teorema 18.74 (pág. 1002 de esta edición)— de orden $\varphi(m)$.

Ejemplo 559

Utilizando el teorema de EULER-FERMAT, demostremos que si n es impar y no es múltiplo ni de 3, ni de 5, entonces $n^{16} - 1$ es múltiplo de 60.

[Cubit 114].

Resolución.— Debemos demostrar que $n^{16} - 1 \equiv 0 \pmod{60}$. Para poder aplicar el teorema de EULER-FERMAT —*cfr. supra* teorema 18.91 (pág. 1013 de esta edición)— deberíamos asegurar que $\text{mcd}(n, 60) = 1$. Veamos; por un lado, sabemos que n no es múltiplo ni de 3 ni de 5 y, por otro lado, como n es impar, n tampoco es múltiplo de 2, así, como $60 = 2^2 \cdot 3 \cdot 5$, tenemos que $\text{mcd}(n, 60) = 1$. Ahora, por el teorema de EULER-FERMAT,

$$n^{\varphi(60)} \equiv 1 \pmod{60},$$

esto es,

$$n^{16} \equiv 1 \pmod{60},$$

es decir,

$$n^{16} - 1 \equiv 0 \pmod{60},$$

en otras palabras, $n^{16} - 1$ es múltiplo de 60. ■

§ 18.10 Resolución de congruencias, II

Aquí tendremos un segundo contacto con la resolución de congruencias lineales.

Teorema 18.92 (Corolario 0.º del teorema de EULER-FERMAT)
$\forall a \in \mathbb{Z}, \forall m \in \mathbb{Z}^+$, si $\text{mcd}(a, m) = 1$, entonces el inverso módulo m de a es $a^{\varphi(m)-1}$.

Demostración.— $a \cdot a^{\varphi(m)-1} = a^{\varphi(m)}$ que según el teorema de EULER-FERMAT es congruente con 1 módulo m. ■

Cuando $\text{mcd}(a, m) = 1$, el siguiente corolario proporciona la solución única módulo m de la congruencia lineal $ax \equiv b \pmod{m}$.

Teorema 18.93 (Corolario 1.º del teorema de EULER-FERMAT)
Si $\text{mcd}(a, m) = 1$, la única solución módulo m de $ax \equiv b \pmod{m}$ es

$$x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

Demostración.— Como $\text{mcd}(a, m) = 1$, por el teorema 18.92 (pág. 1014 de esta edición), el inverso módulo m de a es $a^{\varphi(m)-1}$, y por el teorema 18.83 (pág. 1010 de esta edición), la única solución módulo m es $x \equiv ba^{\varphi(m)-1} \pmod{m}$. ∎

Ejemplo 560

Resolvamos la ecuación

$$5x \equiv 3 \pmod{24}.$$

[Cubit 115].

Resolución.— Apliquemos el corolario 1.º del teorema de EULER-FERMAT —*cfr. supra* teorema 18.93 (pág. 1015 de esta edición)—. Como $\text{mcd}(5, 24) = 1$, entonces existe una única solución módulo 24 que es

$$x \equiv 3 \cdot 5^{\varphi(24)-1}.$$

Calculemos ahora $\varphi(24)$, por ejemplo, usando, por ejemplo, el hecho de que φ es multiplicativa (*cfr. supra* teorema 18.59 —pág. 984—): como $\text{mcd}(3, 8) = 1$, entonces $\varphi(24) = \varphi(3) \cdot \varphi(8) = 2 \cdot 4 = 8$, de donde $x \equiv 3 \cdot 5^7 \pmod{24}$.

Pero esta solución, única módulo 24, no nos debería convencer. ¿Por qué? Porque el resultado debería ser un miembro del menor sistema de residuos módulo 24, $\{0, 1, 2, \ldots, 23\}$. Y eso, ¿por qué? Pensemos en un reloj con las 24 horas «estándar», si nos preguntasen la hora, ¿qué clase de respuesta sería «son las $3 \cdot 5^7$ en punto»?; así que nos interesa saber qué hora «estándar» es las $3 \cdot 5^7$ en punto. Dicho en el lenguaje de congruencias, ¿a qué clase de equivalencia módulo 24 pertenece $3 \cdot 5^7$?

Vamos a ver una forma de trabajar que nos servirá como estrategia inicial para casos más complicados. Necesitamos encontrar un entero x tal que

$$x \equiv 3 \cdot 5^7 \pmod{24} \tag{18.15}$$

y $0 \leq x < 24$. Una forma de hacer las cosas es comenzar con congruencias conocidas y progresar hasta la que buscamos usando propiedades convenientes de congruencias. Una propiedad que nos permite avanzar hacia potencias genéricas es la potencia, ésta es,

$$(\forall a, b \in \mathbb{Z})(\forall m \in \mathbb{Z}^+)(a \equiv b \pmod{m} \to a^n \equiv b^n \pmod{m}),$$

con n entero positivo. Otra, hacia números (en particular, potencias) mayores, la monotonía multiplicativa, ésta es,

$$(\forall a, b \in \mathbb{Z})(\forall m \in \mathbb{Z}^+)(a \equiv b \pmod{m} \rightarrow a \cdot c \equiv b \cdot c \pmod{m}),$$

con c entero. Comencemos:

$$5^2 \equiv 1 \pmod{24} \tag{18.16}$$

es una congruencia conocida (lo es, ya que sabemos que el resto de la división entera de 25 entre 24 es 1), entonces multiplicando por 5^2 en ambos lados (la segunda propiedad que hemos mencionado nos asegura que la congruencia sigue siendo válida), obtenemos

$$5^2 \cdot 5^2 \equiv 5^2 \cdot 1 \pmod{24},$$

esto es,

$$5^4 \equiv 5^2 \pmod{24}. \tag{18.17}$$

Ahora, de (18,17) y (18,16), de la transitividad de la relación de equivalencia $\equiv \pmod{24}$, se sigue que

$$5^4 \equiv 1 \pmod{24}.$$

Continuemos hasta conseguir resolver $3 \cdot 5^7 \equiv x \pmod{24}$. No olvidemos que nuestro objetivo es averiguar qué «representante menor módulo 24» x (esto es, qué miembro x del menor sistema de residuos módulo 24) es congruente con $3 \cdot 5^7$ módulo 24.

El hecho es que partiendo de $5^4 \equiv 1 \pmod{24}$, tenemos que aproximarnos a $3 \cdot 5^7 \equiv x \pmod{24}$, averiguando así x.

Veamos; partiendo de

$$5^4 \equiv 1 \pmod{24}$$

y multiplicando por 5^2 en ambos lados (la segunda propiedad que hemos mencionado nos asegura que la congruencia sigue siendo válida),

$$5^2 \cdot 5^4 \equiv 5^2 \cdot 1 \pmod{24},$$

obtenemos

$$5^6 \equiv 5^2 \pmod{24}$$

y, de nuevo, aplicando la transitiva de $\equiv \pmod{24}$ a esta última y (18.16), obtenemos

$$5^6 \equiv 1 \pmod{24}. \tag{18.18}$$

No olvidemos que lo que queremos averiguar es el menor representante módulo 24 que es congruente con $3 \cdot 5^7$, así que debemos aproximarnos a 5^7. Multiplicando por 5 ambos lados de (18.18) (la

segunda propiedad que hemos mencionado nos asegura que la congruencia sigue siendo válida),

$$5 \cdot 5^6 \equiv 5 \cdot 1 \pmod{24},$$

obtenemos

$$5^7 \equiv 5 \pmod{24},$$

y multiplicando ambos lados de esta última por 3 (la segunda propiedad que hemos mencionado nos asegura que la congruencia sigue siendo válida),

$$3 \cdot 5^7 \equiv 3 \cdot 5,$$

y así, finalmente, de (18,15)y (18,10), por la transitividad de la relación de equivalencia $\equiv \pmod{24}$, obtenemos

$$x \equiv 3 \cdot 5 \pmod{24},$$

esto es,

$$x \equiv 15 \pmod{24},$$

y ésta es la solución, única módulo 24, de la congruencia lineal $5x \equiv 3 \pmod{24}$. ■

Ejemplo 561

Usemos la teoría de relaciones de congruencias para responder a lo siguiente.

0. Demostremos que $21 \cdot 2^{5n+1} - 4 \cdot 3^{3n+1}$ es divisible por 5, para cualquier $n \in \mathbb{N}$.
1. Calculemos el resto de dividir $3^{6n+1} + 3^{2n+1} \cdot 19^{2n} - 3$ entre 28, para cualquier $n \in \mathbb{N}$.

0: [EFE 7.7.2017:3a]; 1: [EFE 7.7.2017:3b], [EFO 20.5.2022:5b], [SEL 7:1]. *Cfr.* González [153]: ejemplo 12.6 (pág. 351).

Resolución.— Veamos.

0. Por un lado:

$$\left.\begin{aligned} 2^5 &= 32 \equiv 2 \pmod 5 \\ 3^3 &= 27 \equiv 2 \pmod 5 \end{aligned}\right\}$$

$$\stackrel{(a)}{\to} \quad 2^5 \equiv 3^3 \pmod 5$$

$$\stackrel{(b)}{\to} \quad 2^{5n} \equiv 3^{3n} \pmod 5 \qquad (1)$$

Por otro:

$$7 \equiv 2 \pmod 5$$

$$\stackrel{(c)}{\to} \quad 7 \cdot 2 \equiv 2 \cdot 2 \pmod 5$$

$$\stackrel{(d)}{\to} \quad 7 \cdot 2 \cdot 3 \equiv 2 \cdot 2 \cdot 3 \pmod 5 \qquad (2)$$

Sustituyendo (2) en (1):

$$7 \cdot 3 \cdot 2 \cdot 2^{5n} \equiv 2 \cdot 2 \cdot 3 \cdot 3^{3n} \pmod 5$$
$$21 \cdot 2^{5n+1} \equiv 4 \cdot 3^{3n+1} \pmod 5$$

lo que por definición de relación de congruencia, significa que $21 \cdot 2^{5n+1} - 4 \cdot 3^{3n+1}$ es divisible por 5.

1. Por un lado:

$$3^3 = 27 \equiv -1 \pmod{28}$$
$$\overset{(e)}{\rightarrow} \quad 3^{6n} = (3^3)^{2n} \equiv (-1)^{2n} = 1 \pmod{28}$$
$$\overset{(d)}{\rightarrow} \quad 3^{6n+1} \equiv 3 \pmod{28} \tag{18.19}$$

Por otro:

$$57 = 3 \cdot 19 \equiv 1 \pmod{28}$$
$$\overset{(e)}{\rightarrow} \quad 3^{2n} \cdot 19^{2n} \equiv 1 \pmod{28}$$
$$\overset{(d)}{\rightarrow} \quad 3^{2n+1} \cdot 19^{2n} \equiv 3 \pmod{28} \tag{18.20}$$

De (18.19) y (18.20), por la propiedad aditiva (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) de las congruencias, sumándolas miembro a miembro:

$$3^{6n+1} + 3^{2n+1} \cdot 19^{2n} \equiv 6 \pmod{28}$$
$$\rightarrow \quad 3^{6n+1} + 3^{2n+1} \cdot 19^{2n} - 3 \equiv 3 \pmod{28}$$

Solución.— El resto de dividir $3^{6n+1} + 3^{2n+1} \cdot 19^{2n} - 3$ entre 28, sea cual sea $n \in \mathbb{N}$, es 3. ■

(a) Por simétrica y transitiva de la relación de congruencia.
(b) Elevando a n ambos miembros.
(c) Multiplicando por 2 ambos miembros.
(d) Multiplicando por 3 cada miembro.
(e) Elevando a $2n$ cada miembro.

Actividad 18.23

Usemos la teoría de relaciones de congruencias para responder a lo siguiente.

0. Demostremos que $3 \cdot 5^{2n+1} + 2^{3n+1}$ es divisible por 17, para cualquier $n \in \mathbb{N}$.
1. Calculemos el resto de dividir $9^{6n+1} + 3^{2n+1} \cdot 487^{2n} - 10$ entre 730, para cualquier $n \in \mathbb{N}$.

0: [AIC 10.4.2018:2Ab], [AIC 10.4.2018:2Bb], [SEL 7:4]. *Cfr.* González [153]: ejemplos 13.9 (pág. 364) y 3.11 (págs. 365–366).

Ejemplo 562

Resolvamos la congruencia lineal $25x \equiv 15 \pmod{120}$.

[AIC 10.4.2018:4B].

Resolución.— Lo primero, deberíamos asegurar que no perdemos el tiempo buscando una solución (imaginemos que la congruencia no tuviese solución). Pues bien, como $d = \text{mcd}(25, 120) = 5$ y $d \mid 15$, del teorema 18.84 (pág. 1010 de esta edición), se sigue que la congruencia tiene solución; ahora, según el teorema 18.85 (pág. 1010 de esta edición), tiene $d = 5$ soluciones módulo 120. De hecho, según este último teorema, debemos considerar la congruencia

$$(25/5)x \equiv (15/5) \pmod{120/5},$$

esto es,

$$5x \equiv 3 \pmod{24}.$$

Observemos que esta congruencia es la que hemos resuelto en el ejemplo 560 (pág. 1015 de esta edición). Su única solución módulo 24 es

$$x \equiv 15 \pmod{24},$$

por lo que, del teorema 18.85 (pág. 1010 de esta edición), se sigue que las cinco soluciones, únicas módulo 120, de $25x \equiv 15 \pmod{120}$ son 15, 39, 63, 87 y 111, esto es,

$$x \equiv 15 + 0 \cdot (120/5) \pmod{120}, \text{ esto es, } x \equiv 15 \pmod{120},$$
$$x \equiv 15 + 1 \cdot (120/5) \pmod{120}, \text{ esto es, } x \equiv 39 \pmod{120},$$
$$x \equiv 15 + 2 \cdot (120/5) \pmod{120}, \text{ esto es, } x \equiv 63 \pmod{120},$$
$$x \equiv 15 + 3 \cdot (120/5) \pmod{120}, \text{ esto es, } x \equiv 87 \pmod{120},$$
$$x \equiv 15 + 4 \cdot (120/5) \pmod{120}, \text{ esto es, } x \equiv 111 \pmod{120}.$$

■

Ejemplo 563

Demostremos que $\forall n \in \mathbb{N}, 10 \mid (3^{4n} + 9)$.

Resolución.—

Vía 0.

De $3^2 \equiv -1 \pmod{10}$ y ella misma, por la propiedad multiplicativa, obtenemos $3^4 \equiv 1 \pmod{10}$, de donde, por la propiedad de la potencia, $3^{4n} \equiv 1^n = 1 \pmod{10}$ y de aquí, por la propiedad aditiva con $9 \equiv 9 \pmod{10}$ [reflexividad de $\pmod{10}$], obtenemos $3^{4n} + 9 \equiv 10 \pmod{10}$,

es decir, $3^{4n}+9\equiv 0 \pmod{10}$ [por transitividad de $\pmod{10}$, de ella y $10\equiv 0 \pmod{10}$], en otras palabras, 10 divide a $3^{4n}+9$. □

Vía 1.

Observemos que vista como una ecuación en congruencias, $(3^{4x}+9)\equiv 0 \pmod{10}$ es no lineal y que lo que pretendemos demostrar es que $\mathbb{N}$ es un subconjunto del conjunto de sus soluciones.

Notando «$10\,|\,(3^{4n}+9)$» por $P(n)$, lo que se propone es demostrar que $\forall n\in\mathbb{N}, P(n)$. Para conseguirlo, apliquemos inducción débil[36]:

Caso base (ID_0).— Si $n=0, 3^0+9=1+9=10\in M(10)$, por lo que $P(0)$ es cierta.

Hipótesis inductiva.— Supongamos $P(k)$ cierta, es decir, suponemos que $10\,|\,(3^{4k}+9)$ es verdad.

Paso inductivo (ID_1).— Demostremos que $P(k)$ implica $P(k+1)$, esto es, que de $10\,|\,(3^{4k}+9)$ se sigue que $10\,|\,(3^{4(k+1)}+9)$; en efecto, por un lado,

$$\begin{aligned} 10\,|\,(3^{4k}+9) &\to 10\,|\,3^4\cdot(3^{4k}+9) \qquad \text{(si } a \text{ divide a } b\text{, } a \text{ divide a cualquier múltiplo de } b\text{)}\\ &\to 10\,|\,(3^{4k+4}+3^4\cdot 9)\\ &\to 10\,|\,(3^{4k+4}+729)\\ &\to 10\,|\,(3^{4(k+1)}+9+720), \end{aligned}$$

y por esto hemos multiplicado antes precisamente por 3^4, porque, por otro lado, como $10\,|\,720$, necesariamente $10\,|\,(3^{4(k+1)}+9)$, es decir, se tiene $P(k+1)$.

Conclusión ($\mathrm{ID}_0\wedge\mathrm{ID}_1$).— Como se satisfacen el caso base y el paso inductivo, entonces, por el teorema de inducción débil[36], se tiene lo buscado, a saber, que $\forall n\in\mathbb{N}, 10\,|\,(3^{4n}+9)$, en otras palabras, $\mathbb{N}$ es un subconjunto del conjunto de soluciones de la ecuación en congruencias no lineal $(3^{4x}+9)\equiv 0 \pmod{10}$. ■

§ 18.11 El teorema pequeño de FERMAT

Teorema 18.94 (Corolario 2.º del teorema de EULER-FERMAT)
$(\forall a,p\in\mathbb{Z}, p \text{ primo})\ (p\nmid a\to a^{p-1}\equiv 1 \pmod{p})$.

Observación 18.11.0.— Análogamente a lo dicho en la observación 18.9.1 (pág. 1014 de esta edición), pudiésemos ver este corolario 2.º del teorema de EULER-FERMAT como corolario de ser $\langle\mathbb{Z}_p^\times;\cdot\rangle$ un grupo —*cfr. supra* teorema 18.74 (pág. 1002 de esta edición)— de orden $p-1$.

[36] *Cfr. supra* teorema 16.0 (pág. 805).

Ejemplo 564

Demostremos que 20^6 tiene la forma de un múltiplo de 7 más 1.

[Cubit 116].

Resolución.— Tener 20^6 la forma de un múltiplo de 7 más 1, lo expresamos con congruencias por

$$20^6 \equiv 1 \pmod 7.$$

Esto es lo que debemos demostrar.

El número 7 es un primo que no divide a 20, entonces, por el corolario 2.º del teorema de EULER-FERMAT,

$$20^{7-1} \equiv 1 \pmod 7,$$

esto es,

$$20^6 - 1 \equiv 0 \pmod 7,$$

es decir,

$$20^6 - 1 \text{ es múltiplo de } 7,$$

en otras palabras, 20^6 tiene la forma de un múltiplo de 7 más 1. ■

Teorema 18.95 (Teorema pequeño de FERMAT)
$(\forall a, p \in \mathbb{Z}, p \text{ primo})\ (a^p \equiv a \pmod p)$.

Observación 18.11.1.— El teorema pequeño de FERMAT muestra una condición necesaria, aunque no suficiente, para que un número sea primo. En efecto: 10 no es primo porque existe $a \in \mathbb{Z}$, digamos $a = 2$, tal que $2^{10} = 1024 \equiv 4 \pmod{10}$, esto es, $2^{10} \equiv 4 \not\equiv 2 \pmod{10}$, pero 2 puede que sea primo porque $(\forall n \in \mathbb{Z})\ (2n)^2 \equiv 0 \pmod 2$ y $(2n+1)^2 \equiv 1 \pmod 2$.[37]

Observación 18.11.2.— Un enunciado equivalente del teorema pequeño de FERMAT es: $(\forall a, p \in \mathbb{Z}$, p primo) $p \mid (a^p - a)$.

Teorema 18.96
Si $\operatorname{mcd}(a, p) = 1$, entonces el corolario 2.º del teorema de EULER-FERMAT y el teorema pequeño de FERMAT son equivalentes.

[37] Para esto último, *cfr. supra* ejemplo 18.2 (pág. 952 de esta edición).

Demostración.— Si $p \nmid a$, entonces $a \cdot a^{p-1} \equiv a \cdot 1 \pmod{p}$ [producto por un escalar], esto es, $a^p \equiv a \pmod{p}$; si $p \mid a$, entonces $a \equiv 0 \pmod{p}$, de donde $a^p \equiv 0 \pmod{p}$ [potencia] y $0 \equiv a \pmod{p}$ [simétrica], por lo que $a^p \equiv a \pmod{p}$ [transitiva].

Recíprocamente, como $a^p = a^{p-1} \cdot a \equiv 1 \cdot a \pmod{p}$, entonces $a^{p-1} \equiv 1 \pmod{p}$ [simplificación primal[38], por ser p primo y $p \nmid a$]. ■

Ejemplo 565

Usando la teoría de relaciones de congruencia, demostremos que 7 divide a $1111^{2222} + 2222^{1111}$.

Sugerencia.— Demostremos que $1111 \equiv 5 \pmod 7$ y que $2222 \equiv 3 \pmod 7$; para ello, usemos que $1111 = 10^3 + 10^2 + 10^1 + 10^0$ y que $2222 = 2 \cdot 1111$. Finalmente, apliquemos el teorema de EULER-FERMAT para intentar hacer que las potencias caigan en picado.

[SEL 7:5]. *Cfr.* ABELLANAS y GALINDO [207]: ejercicio 1.5 (pág. 14).

Resolución.— Veamos. Por un lado,

$$10^0 \equiv 1 \pmod{7}, \tag{18.21}$$
$$10^1 \equiv 3 \pmod{7}. \tag{18.22}$$

Calculemos ahora la congruencia correspondiente a 10^2 mediante una estrategia general por la propiedad multiplicativa aplicada a (18.22) consigo misma,

$$10^1 \cdot 10^1 \equiv 3 \cdot 3 \pmod{7},$$

y aplicando la transitiva de $\equiv \pmod{7}$ a ésta y a $3^2 \equiv 2 \pmod{7}$, obtenemos

$$10^2 \equiv 2 \pmod{7}, \tag{18.23}$$

Usemos la misma estrategia para calcular la congruencia correspondiente a 10^3 de nuevo por la propiedad multiplicativa aplicada esta vez a (18.22) y (18.23),

$$10^1 \cdot 10^2 \equiv 3 \cdot 2 \pmod{7},$$

y aplicando la transitiva de $\equiv \pmod{7}$ a ésta y a $6 \equiv -1 \pmod{7}$, obtenemos

$$10^3 \equiv -1 \pmod{7}. \tag{18.24}$$

[38] *Cfr. supra* teorema 18.69 (pág. 997 de esta edición).

En lo que sigue, de las propiedades de las congruencias, utilizaremos la aditiva, el producto por escalar entero y la potencia.[39]

Ahora, al ser $1111 = 1 \cdot 10^3 + 1 \cdot 10^2 + 1 \cdot 10^1 + 1 \cdot 10^0$ (nos lo sugieren), entonces, por la propiedad aditiva de las congruencias, aplicada reiteradamente a (18.21), (18.22), (18.23) y (18.24),

$$10^3 + 10^2 + 10^1 + 10^0 \equiv -1 + 2 + 3 + 1 \pmod{7},$$

esto es,

$$1111 \equiv 5 \pmod{7},$$

de donde, por la propiedad producto por escalar entero, multiplicando por 2 en ambos lados,

$$2 \cdot 1111 \equiv 2 \cdot 5 \pmod{7},$$

y aplicando la transitiva de la relación $\equiv \pmod{7}$ a ésta y a $10 \equiv 3 \pmod{7}$, obtenemos

$$2222 \equiv 3 \pmod{7}.$$

Ahora, por la propiedad potencia de las congruencias,

$$1111 \equiv 5 \pmod{7} \to 1111^{2222} \equiv 5^{2222} \pmod{7},$$
$$2222 \equiv 3 \pmod{7} \to 2222^{1111} \equiv 3^{1111} \pmod{7},$$

y, de nuevo, por la propiedad aditiva,

$$1111^{2222} + 2222^{1111} \equiv 5^{2222} + 3^{1111} \pmod{7} \tag{18.25}$$

Por otro lado, por el corolario 2.º del teorema de Euler-Fermat[40], como 7 es primo y 5 no es múltiplo de 7, se tiene que

$$5^{7-1} = 5^6 \equiv 1 \pmod{7}, \tag{18.26}$$

y como 3 no es múltiplo de 7, también que

$$3^{7-1} = 3^6 \equiv 1 \pmod{7},$$

de ésta, por la simetría de la relación de equivalencia $\equiv \pmod{7}$,

$$1 \equiv 3^6 \pmod{7}. \tag{18.27}$$

[39] *Vid. supra* teorema 18.68 (pág. 992 de esta edición).
[40] *Vid. supra* teorema 18.94 (pág. 1020 de esta edición).

Aplicando la transitividad de la relación de equivalencia $\equiv \pmod 7$ a (18.26) y (18.27), obtenemos

$$5^6 \equiv 3^6 \pmod 7.$$

Observemos también que por la propiedad potencia de las congruencias,

$$5^6 \equiv 1 \pmod 7 \to (5^6)^n \equiv 1 \pmod 7, \text{ para todo } n \in \mathbb{N},$$
$$3^6 \equiv 1 \pmod 7 \to (3^6)^m \equiv 1 \pmod 7, \text{ para todo } m \in \mathbb{N}.$$

Además, como $1111 = 185 \cdot 6 + 1$ y $2222 = 370 \cdot 6 + 2$ (esto es, $1111 \equiv 1 \pmod 6$ y $2222 \equiv 2 \pmod 6$), entonces

$$3^{1111} = (3^6)^{185} \cdot 3^1,$$
$$5^{2222} = (5^6)^{370} \cdot 5^2.$$

Ahora bien, de $(5^6)^{370} \equiv 1 \pmod 7$ (de la observación en el penúltimo párrafo, en particular para $n = 370$), por la propiedad producto por escalar entero,

$$5^{2222} = (5^6)^{370} \cdot 5^2 \equiv 5^2 \pmod 7, \tag{18.28}$$

y de $(3^6)^{185} \equiv 1 \pmod 7$, de nuevo por la propiedad producto por escalar entero,

$$3^{1111} = (3^6)^{185} \cdot 3^1 \equiv 3^1 \pmod 7. \tag{18.29}$$

De (18.28) y (18.29), por la propiedad aditiva de las congruencias, sumándolas miembro a miembro,

$$5^{2222} + 3^{1111} \equiv 5^2 + 3^1 \pmod 7, \tag{18.30}$$

y, por tanto, de (18.25) y (18.30), por la transitividad de $\equiv \pmod 7$, obtenemos

$$1111^{2222} + 2222^{1111} \equiv 5^2 + 3^1 \pmod 7, \tag{18.31}$$

y como $5^2 + 3^1 = 28$ y

$$28 \equiv 0 \pmod 7, \tag{18.32}$$

por la transitividad de $\equiv \pmod 7$ aplicada a (18.31) y (18.32),

$$1111^{2222} + 2222^{1111} \equiv 0 \pmod 7,$$

en otras palabras, $1111^{2222} + 2222^{1111}$ es múltiplo de 7. ■

§ 18.12 Congruencias (polinómicas) módulo primo

Teorema 18.97 (Teorema de WILSON, 1770)
$(\forall p \in \mathbb{Z}, p \text{ primo}) \, ((p-1)! \equiv -1 \pmod{p})$. (congruencia de WILSON)

Observación 18.12.0.— Éste resultado conocido ahora por teorema de WILSON ya lo utilizaba ALHACÉN en sus demostraciones.[41]

Teorema 18.98 (Recíproco del teorema de WILSON, 1770)
$(\forall n \in \mathbb{Z}, n > 1) \, ((n-1)! \equiv -1 \pmod{n} \to n \text{ es primo})$.

Observación 18.12.1.— Si bien podría utilizarse el recíproco del teorema de WILSON como criterio de primalidad, es poco práctico, pues el factorial crece muy rápido.

Teorema 18.99 (Teorema de WOLSTENHOLME, 1862)
$(\forall p \in \mathbb{Z}, p \text{ primo}, p \geq 5) \binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ —o, equivalentemente, como el par de congruencias $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2}$ y $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p}$—.

Observación 18.12.2.— Por cierto, actualmente:

- se conjetura que existen infinitos *primos de* WILSON, siendo éstos aquellos primos p cuyo cuadrado divide a $(p-1)! + 1$ —a fecha de hoy sólo se conocen tres: 5, 13 y 563—;[42]
- se conjetura que existen infinitos *primos de* WOLSTENHOLME, siendo éstos aquellos primos $p > 7$ tales que $\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$ —a fecha de hoy sólo se conocen dos: 16 843 y 2 124 679—;[43]
- se desconoce si algún número compuesto satisface el teorema de WOLSTENHOLME.

Ejemplo 566

Demostremos que $112! + 97^{112}$ es múltiplo de 113.

[Cubit 117].

[41] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Ibn_al-Haytham.
[42] *Vid. v. gr.* https://oeis.org/A007540.
[43] *Vid. v. gr.* https://oeis.org/A088164.

Resolución.— El número 113 es primo, entonces, por el teorema de WILSON,

$$(113-1)! \equiv -1 \pmod{113}. \tag{18.33}$$

Por otro lado, como 113 es un número primo que no divide a 97, entonces, por el corolario 2.º del teorema de EULER-FERMAT,

$$97^{113-1} \equiv 1 \pmod{113}. \tag{18.34}$$

De (18.33) y (18.34), por la propiedad aditiva[44] de las congruencias, sumándolas miembro a miembro,

$$(113-1)! + 97^{113-1} \equiv -1+1 \pmod{113},$$

esto es,

$$112! + 97^{112} \equiv 0 \pmod{113},$$

es decir,

$$112! + 97^{112} \text{ es múltiplo de } 113.$$ ■

§ 18.13 Congruencias lineales simultáneas

Ejemplo 567

En un ensayo de una banda de música sucede que: tanto si desfilan de 4 en 4, como si lo hacen de 3 en 3 o de 2 en 2, sobra una persona (en la última fila sólo hay una persona), pero si desfilan de 5 en 5, no sobra ni falta nadie (en todas las filas hay 5 personas). ¿Cuántas personas componen la banda si son menos de 100 personas?

[Cubit 124].

Resolución.— Formalicemos la situación con congruencias. Veamos; si desfilan de 4 en 4, sobra una persona (en la última fila sólo hay una persona), esto quiere decir que al dividir el número total de personas x entre 4, el resto es 1, en lenguaje de congruencias,

$$x \equiv 1 \pmod{4};$$

similarmente, si desfilan de 3 en 3, sobra una persona, esto es,

$$x \equiv 1 \pmod{3};$$

[44] *Vid. supra* teorema 18.68 (pág. 992 de esta edición).

si desfilan de 2 en 2, sobra una persona, es decir,

$$x \equiv 1 \pmod{2}.$$

Tenemos así el sistema de congruencias lineales

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{2} \end{cases}$$

Este sistema no es complicado de resolver. Usando la definición de congruencia, reescribimos el sistema de esta forma:

$$\begin{cases} x - 1 \equiv 0 \pmod{4} \\ x - 1 \equiv 0 \pmod{3} \\ x - 1 \equiv 0 \pmod{2} \end{cases}$$

Este sistema nos informa de que

$$x - 1 \text{ es múltiplo de } 2, 3 \text{ y } 4,$$

así que,

$$x - 1 \text{ es múltiplo del mínimo común múltiplo de } 2, 3 \text{ y } 4,$$

es decir,

$$x - 1 \text{ es múltiplo de } 12,$$

esto es,

$$\exists n \in \mathbb{Z}, x = 12n + 1$$

—en lenguaje de congruencias, $x \equiv 1 \pmod{12}$—, por lo que sumando 1 a cada múltiplo de 12 menor que 100 (la banda tiene menos de 100 personas), resulta que se trata de

$$13, 25, 37, 49, 61, 73, 85 \text{ o } 97 \text{ personas.}$$

Y como nos dicen que si desfilan de 5 en 5 no sobra ni falta nadie, el número de personas es múltiplo de 5, por tanto, hay dos posibles soluciones, 25 u 85 personas. ■

Ejemplo 568

(Variante del ejemplo 567 [pág. 1026]). En un ensayo de una banda de música sucede que: si desfilan de 2 en 2, de 3 en 3 o de 4 en 4, entonces falta una persona en la última fila (hay un hueco), pero si desfilan de 5 en 5, no falta ni sobra nadie (en todas las filas hay 5 personas). ¿Cuántas personas componen la banda si no son más de 100 personas?

[Cubit 125].

Resolución.— Para darnos cuenta de lo que significa «faltar», escribamos el sistema en términos de «sobrar», en vez de «faltar», así, al desfilar de 4 en 4, faltar 1 equivale a sobrar 3,

$$x \equiv 3 \pmod 4,$$

esto es,

$$x \bmod 4 = 3 \bmod 4, \tag{18.35}$$

pero también se tiene que

$$3 \bmod 4 = -1 \bmod 4; \tag{18.36}$$

ahora, de (18,35) y (18,36), por la transitiva de la igualdad,

$$x \bmod 4 = -1 \bmod 4,$$

esto es,

$$x \equiv -1 \pmod 4;$$

mediante un razonamiento similar para los casos de desfilar de 3 en 3 y de 2 en 2, tenemos que

$$x \equiv -1 \pmod 3 \qquad \text{y} \qquad x \equiv -1 \pmod 2.$$

Tenemos así el sistema de congruencias lineales

$$\begin{cases} x \equiv -1 \pmod 4 \\ x \equiv -1 \pmod 3 \\ x \equiv -1 \pmod 2 \end{cases}$$

que resolvemos siguiendo la idea del ejemplo 567 (pág. 1026 de esta edición), esto es, usando la definición de congruencia, reescribimos el sistema en la forma:

$$\begin{cases} x + 1 \equiv 0 \pmod 4 \\ x + 1 \equiv 0 \pmod 3 \\ x + 1 \equiv 0 \pmod 2 \end{cases}$$

Este sistema nos informa de que

$$x + 1 \text{ es múltiplo de } 2, 3 \text{ y } 4,$$

así que,

$$x + 1 \text{ es múltiplo del mínimo común múltiplo de } 2, 3 \text{ y } 4,$$

es decir,

$$x + 1 \text{ es múltiplo de } 12,$$

esto es,

$$\exists n \in \mathbb{Z}, x = 12n - 1$$

—en lenguaje de congruencias, $x \equiv 11 \pmod{12}$—, por lo que restando 1 a cada múltiplo de 12 no mayor que 100 (la banda no tiene más de 100 personas), resulta que se trata de

11, 23, 35, 47, 59, 71, 83 o 95 personas.

Y como nos dicen que si desfilan de cinco en cinco no falta ni sobra nadie, el número de personas es múltiplo de 5, por tanto, hay dos posibles soluciones, 35 u 95 personas. ■

Actividad 18.24

Resolvamos: $\begin{cases} x + 2y \equiv 4 \pmod{7} \\ 4x + 3y \equiv 4 \pmod{7} \end{cases}$

[AIC 10.4.2018:4A].

Actividad 18.25

Dos personas llevaban un cesto de huevos. Un caballo que pasó a su lado hizo un extraño y les asustó, cayéndose el cesto y rompiéndose todos los huevos. La persona al cargo del caballo, queriendo pagarles su pérdida, les preguntó cuántos huevos llevaban en el cesto. Ellas no se acordaban exactamente aunque recuerdan que al contarlos en manos de tres sobraban dos y en manos de cuatro, sobraban tres. Calcule el número de huevos, sabiendo que estaba entre 100 y 110, utilizando la teoría de las ecuaciones en congruencias.

[EFO 1.6.2017:3b], [SEL 7:2]. *Cfr.* González [153]: ejemplo 12.6 (pág. 351).

§ 18.13.0 Teorema chino de los restos

Teorema 18.100 (Teorema chino de los restos)
Sean $m_0, m_1, \ldots, m_k$ primos dos a dos, sea $M = m_0 \cdot m_1 \cdot \ldots \cdot m_k$ y sean $b_0, b_1, \ldots, b_k$ enteros cualesquiera, entonces el sistema de congruencias lineales

$$\begin{cases} x \equiv b_0 \pmod{m_0}, \\ x \equiv b_1 \pmod{m_1}, \\ \quad \vdots \\ x \equiv b_k \pmod{m_k}. \end{cases}$$

tiene una única solución módulo M (es decir, cualquier otra solución es congruente módulo M con ésta) que es

$$x \equiv b_0 M_0 M_0' + b_1 M_1 M_1' + \ldots + b_k M_k M_k' \pmod{M}$$

siendo para todo $i \in \mathbb{N}_{<k+1}$, $M_i = M/m_i$ y M_i' el inverso único de M_i módulo m_i, esto es, la única solución de $M_i x \equiv 1 \pmod{m_i}$, solución que existe por ser $\operatorname{mcd}(M_i, m_i) = 1$.

Ejemplo 569

Sea n un número entero positivo menor que 60 y sean a, b y c los restos de dividir n entre 3, 4 y 5, respectivamente; utilicemos el teorema chino de los restos para demostrar que n es el resto de dividir $40a + 45b + 36c$ entre 60.

[EFE 29.6.2018:3].

Resolución.— En esta ocasión, m_1, m_2 y m_3 son los enteros positivos 3, 4 y 5, respectivamente, que son coprimos dos a dos. Por otra parte, $M = 3 \cdot 4 \cdot 5 = 60$. Así:

$$y_1 \frac{60}{3} \equiv 1 \pmod{3} \leftrightarrow 20y_1 \equiv 1 \pmod{3} \to y_1 = 2 \qquad [20 \cdot 2 = 40 \equiv 1 \pmod{3}]$$
$$y_2 \frac{60}{4} \equiv 1 \pmod{4} \leftrightarrow 15y_2 \equiv 1 \pmod{4} \to y_2 = 3 \qquad [15 \cdot 3 = 45 \equiv 1 \pmod{4}]$$
$$y_3 \frac{60}{5} \equiv 1 \pmod{5} \leftrightarrow 12y_3 \equiv 1 \pmod{5} \to y_3 = 3 \qquad [12 \cdot 3 = 36 \equiv 1 \pmod{5}]$$

Por el teorema chino de los restos,

$$\begin{aligned} n &\equiv \left(a \cdot 2 \cdot \frac{60}{3} + b \cdot 3 \cdot \frac{60}{4} + c \cdot 3 \cdot \frac{60}{5} \right) \pmod{60} \\ &\equiv (40a + 45b + 36c) \pmod{60}, \end{aligned}$$

es decir,

$$n \mod 60 = (40a + 45b + 36c) \mod 60,$$

de donde, como $n = n \mod 60$ [por ser $n < 60$],

$$n = (40a + 45b + 36c) \mod 60.$$ ■

Actividad 18.26

(Matemagia [adivinación y mentalismo]).— Pedimos a alguien que piense un número menor que 30. Lo adivinaremos. Para ello, debe decirnos los restos del número que ha pensado al dividirlo por 2, 3 y 5. ¿Qué fórmula debemos conocer para poder dar la respuesta?

[Cubit 120].

Ejemplo 570

Dados los n primeros números primos consecutivos, $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7$, $p_5 = 11$, $p_6 = 13, \ldots, p_n$, ¿cuáles son los números naturales cuya división entera por p_1 da resto 1, por p_2 da resto 2, por p_3 da resto 3, ..., por p_n da resto n?

Resolución.— Ésta es una cuestión clásica que puede resolverse con el teorema chino de los restos.

Por ejemplo, si $n = 3$, entonces los números buscados son $23, 53, 83, \ldots$, esto es, $23 + 30k$, para $k = 0, 1, 2, 3, \ldots$, ya que $1 = 23 \text{ mód } 2 = 53 \text{ mód } 2 = 83 \text{ mód } 2 = \ldots$, $2 = 23 \text{ mód } 3 = 53 \text{ mód } 3 = 83 \text{ mód } 3 = \ldots$ y $3 = 23 \text{ mód } 5 = 53 \text{ mód } 5 = 83 \text{ mód } 5 = \ldots$, esto es, $(23 + 30k) \text{ mód } 2 = 1$, $(23 + 30k) \text{ mód } 3 = 2$ y $(23 + 30k) \text{ mód } 5 = 3$.

Pensar sobre esto pudiese ayudarnos a comprender el teorema chino de los restos. ■

Teorema 18.101 (Teorema chino de los restos, extensión I)

Sean $m_0, m_1, \ldots, m_k$ primos dos a dos, sea $M = m_0 \cdot m_1 \cdot \ldots \cdot m_k$, sean $b_0, b_1, \ldots, b_k$ enteros cualesquiera y sean $a_0, a_1, \ldots, a_k$ enteros tales que $\operatorname{mcd}(a_i, m_i) = 1$ —por lo que cada a_i admite un inverso único a'_i—, entonces el sistema de congruencias lineales

$$\begin{cases} a_0 x \equiv b_0 \pmod{m_0}, \\ a_1 x \equiv b_1 \pmod{m_1}, \\ \quad\vdots \\ a_k x \equiv b_k \pmod{m_k}, \end{cases}$$

es equivalente al sistema

$$\begin{cases} x \equiv b_0 a'_0 \pmod{m_0}, \\ x \equiv b_1 a'_1 \pmod{m_1}, \\ \quad\vdots \\ x \equiv b_k a'_k \pmod{m_k}, \end{cases}$$

al que puede aplicarse el teorema chino de los restos.

Teorema 18.102 (Teorema chino de los restos, extensión II)

Si $m_0, m_1, \ldots, m_k$ son primos dos a dos y $M = m_0 \cdot m_1 \cdot \ldots \cdot m_k$, entonces la ecuación

$$x \equiv n \pmod{M}$$

es equivalente al sistema

$$\begin{cases} x \equiv n \pmod{m_0}, \\ x \equiv n \pmod{m_1}, \\ \quad\vdots \\ x \equiv n \pmod{m_k}. \end{cases}$$

Actividad 18.27

Resolvamos el sistema $x \equiv 5 \pmod{6}$, $x \equiv 8 \pmod{21}$.

[Cubit 121].

Con miras a su resolución.— Por el teorema chino de los restos, extensión II, la ecuación $x \equiv 5 \pmod{6}$ es equivalente al sistema $\{x \equiv 5 \pmod{2}; x \equiv 5 \pmod{3}\}$ y la ecuación $x \equiv 8 \pmod{21}$ es equivalente al sistema $\{x \equiv 8 \pmod{3}; x \equiv 8 \pmod{7}\}$; como $5, 8 \in [2]_3$, $x \equiv 5 \pmod{3}$ es equivalente a $x \equiv 8 \pmod{3}$ y a $x \equiv 2 \pmod{3}$, por lo que el sistema del enunciado es equivalente al sistema

$\{x \equiv 5 \pmod 2; x \equiv 2 \pmod 3; x \equiv 8 \pmod 7\}$, que al ser 2, 3 y 7 primos dos a dos, es resoluble por el teorema chino de los restos.

Actividad 18.28

¿Tiene solución el sistema formado por el anterior y la ecuación $x \equiv 3 \pmod{12}$?

[Cubit 122].

§ 18.14 Criterios de divisibilidad

Definición 18.33.— Decimos que $r \in \mathbb{Z}$ es el *resto potencial de grado* $k \in \mathbb{N}$ (o, sinónimamente, el *kaésimo resto potencial*) *de* x *módulo* m (o, sinónimamente, de x respecto de m), precisamente si es una solución de la ecuación de congruencia $x^k \equiv r \pmod m$.

Definición 18.34.— Dados $b, m \in \mathbb{Z}^+$, los *restos potenciales sucesivos de* b *módulo* m son los números $r_0, r_1, \ldots, r_k$ tales que $b^0 \equiv r_0 \pmod m$, $b^1 \equiv r_1 \pmod m$, ..., $b^k \equiv r_k \pmod m$.

Observación 18.14.0.— Sucede que:

0. los restos potenciales sucesivos de b módulo m son las clases de equivalencia de restos $[b^k]$ módulo m de las sucesivas potencias de b: $[b^0]$, $[b^1]$, $[b^2]$, . . .;
1. una vez obtenemos un resto potencial sucesivo igual a otro anterior, los restos comienzan a repetirse de forma periódica, esto es, si $r_t = r_{t+p}$, entonces la sucesión de restos potenciales sucesivos es $r_0, r_1, \ldots, r_{t-1}, r_t, \ldots, r_{t+p-1}, r_t, \ldots, r_{t+p-1}, \ldots$;
2. el número de restos potenciales sucesivos distintos de b respecto de m es como máximo $m-1$, esto es, $t+p < m$ con los $t+p$ restos $r_0, r_1, \ldots, r_{t+p-1}$ módulo m, todos distintos;
3. no hay restos en la parte no periódica si, y sólo si, b y m son primos entre sí.

Teorema 18.103 (Cálculo de los restos potenciales sucesivos)
Si $b^i \equiv r_i \pmod m$ y $b^j \equiv r_j \pmod m$, entonces $b^{i+j} \equiv r_i r_j \pmod m$.

Demostración.— Por la propiedad multiplicativa de las congruencias. ■

Teorema 18.104 (Criterio general de divisibilidad en base decimal)
Dados $m, n \in \mathbb{Z}^+$, n escrito en forma polinómica en base 10, $n = n_0 + n_1 \cdot 10 + n_2 \cdot 10^2 + \cdots + n_k \cdot 10^k$, entonces n es divisible por m si, y sólo si, $(n_0 r_0 + n_1 r_1 + n_2 r_2 + \cdots + n_k r_k)$ es divisible por m, siendo $r_0, r_1, \ldots, r_k$ los restos potenciales sucesivos de 10 módulo m.

Es éste un caso particular del siguiente, el criterio general de divisibilidad en cualquier base.

Teorema 18.105 (Criterio general de divisibilidad en cualquier base (CGD))
Dados $m, n \in \mathbb{Z}^+$, n escrito en forma polinómica en base b, $n = n_0 + n_1 \cdot b + n_2 \cdot b^2 + \cdots + n_k \cdot b^k$, entonces n es divisible por m en base b si, y sólo si, $(n_0 r_0 + n_1 r_1 + n_2 r_2 + \cdots + n_k r_k)$ es divisible por m en base 10, siendo $r_0, r_1, \ldots, r_k$ los restos potenciales sucesivos de b módulo m.

[EFE 19.1.2023:5a], [EFO 24.5.2023:5a], [EFO 27.5.2025:5a], [EFE 18.6.2025:5a].

§ 18.14.0 Muestra de ejemplos

Ejemplo 571

Queremos:

0. usando el criterio general de divisibilidad, hallar el criterio de divisibilidad por cinco en el sistema de numeración nonario (base nueve);
1. utilizar el criterio de divisibilidad hallado para averiguar si el número nonario $33333_{(9}$ es divisible por cinco;
2. si no lo fuese, usar el criterio de divisibilidad hallado para averiguar para qué cifras nonarias x, el número nonario $33x33_{(9}$ es divisible por cinco.

[EFE 29.6.2018:4].

Resolución.—

0. Sea $n_{(9} = n_k \ldots n_2 n_1 n_0$ un número nonario de $k+1$ cifras, esto es, $n_{(9} = \sum_{i=0}^{k} 9^i n_i$, con $n_i \in \{0, 1, 2, \ldots, 8\}$ y $n_k \neq 0$.

Para poder aplicar el criterio general de divisibilidad en el sistema de numeración nonario[45], calculemos primero los restos potenciales sucesivos de 9 módulo 5.

Al ser

$$9^0 = 1 \equiv 1 \pmod{5},$$
$$9^1 \equiv 4 \equiv -1 \pmod{5},$$
$$9^2 = 9 \cdot 9 \equiv 4 \cdot 4 = 16 \equiv 1 \pmod{5}, \qquad \text{[prop. multiplicativa]}$$

esto es, $r_2 = r_0$, es decir, los restos comienzan a repetirse de forma periódica, por lo que los restos potenciales sucesivos de 9 módulo 5, $r_0, r_1, r_2, \ldots$, son, bien $1, 4, 1, 4, 1, 4, 1, 4, \ldots$, bien $1, -1,$

[45] El *sistema de numeración nonario* (o, sinónimamente, *nonal*) tiene nueve como su base (*vid. v. gr.* https://en.wikipedia.org/wiki/Nonary).

$1, -1, 1, -1, 1, -1, \ldots$, bien cualquier mezcla, por ejemplo, $1, 4, 1, 4, 1, -1, 1, 4, \ldots$ —observemos que no hay residuos en la parte no periódica porque 9 y 5 son primos entre sí—.

Aplicando ahora el criterio general de divisibilidad en base 9, $n_{(9} = n_k \ldots n_2 n_1 n_0$ es divisible por 5 en el sistema de numeración nonario si, y sólo si, $n_0 r_0 + n_1 r_1 + n_2 r_2 + \ldots + n_k r_k$ es divisible por 5 en el sistema de numeración decimal, esto es,

$$n_{(9} \,|_{(9} 5 \leftrightarrow 5 \,|\, (n_0 + 4n_1 + n_2 + 4n_3 + \ldots + b)\,, \text{ donde } b = n_k \ (k \text{ par}) \text{ o } b = 4n_k \ (k \text{ impar}),$$

o bien, eligiendo el segundo conjunto de restos,

$$n_{(9} \,|_{(9} 5 \leftrightarrow 5 \,|\, \left(n_0 - n_1 + n_2 - n_3 + \ldots + (-1)^k n_k\right),$$

y éste es un criterio de divisibilidad por 5 en base 9 —el obtenido mediante el criterio general de divisibilidad en base 9—, en palabras,

> un número nonario es divisible por 5 si, y sólo si, su cifra de lugar cero menos su cifra de lugar uno más su cifra de lugar dos menos su cifra de lugar tres, y así sucesivamente, es divisible por 5;

o, también, y quizás más sencillo de recordar,

> un número nonario es divisible por 5 si, y sólo si, la suma de sus cifras de lugar par menos la suma de sus cifras de lugar impar es divisible por 5.

1. El número $33333_{(9}$ no es divisible por 5 en el sistema de numeración nonario, ya que $3 - 3 + 3 - 3 + 3 = 3$ no es divisible por 5 en el sistema de numeración decimal.

2. Para que $33x33_{(9}$ sea divisible por 5 en el sistema de numeración nonario debe ocurrir que $3-3+x-3+3 = x$ sea divisible por 5 en el sistema de numeración decimal; como $x \in \{0, 1, 2, \ldots, 8\}$, sólo hay dos cifras nonarias que lo hacen divisible por 5, a saber, 0 o 5, por lo que los números son $33033_{(9}$ y $33533_{(9}$. ■

Observación 18.14.1.— Considerando la sucesión de restos potenciales $1, 4, 1, 4, 1, 4, 1, 4, \ldots$, tendríamos un segundo criterio también construido utilizando el criterio general de divisibilidad, a saber,

> un número nonario es divisible por 5 si, y sólo si, la suma de sus cifras de lugar par más cuatro veces la suma de sus cifras de lugar impar es divisible por 5.

Así, $33333_{(9}$ no es divisible por 5 en el sistema de numeración nonario, ya que $3+4\cdot3+3+4\cdot3+3 = 33$ no es divisible por 5 en el sistema de numeración decimal.

Por otra parte, para que $33x33_{(9}$ sea divisible por 5 en el sistema de numeración nonario debe ocurrir que $3 + 4 \cdot 3 + x + 4 \cdot 3 + 3 = 30 + x$ sea divisible por 5 en el sistema de numeración decimal; como $5|30$, todo depende de x, discusión que ya hicimos en el apartado 2 del ejemplo, obteniendo los números $33033_{(9}$ y $33533_{(9}$.

Observación 18.14.2.— También pudiésemos partir de otra cualquiera de las infinitas sucesiones de restos potenciales, por ejemplo, de $1, 4, 1, -1, 1, -1, 1, 4, \ldots$, si bien debemos tener presente que estamos construyendo criterios para ser enunciados y recordados fácilmente, pareciéndonos los más sencillos los dos anteriores ya enunciados.

Ejemplo 572

Usando el criterio general de divisibilidad, hallemos un criterio de divisibilidad por 7 en el sistema de numeración duodecimal (base 12).

[EFE 7.7.2021:5b].

Resolución.— Sea $n_{(12} = \ldots n_3 n_2 n_1 n_0$. Para utilizar el criterio general de divisibilidad debemos calcular los restos potenciales de 12, módulo 7. Multiplicando sucesivamente las congruencias miembro a miembro (propiedad de multiplicación), se tiene:

$$
\begin{aligned}
12^0 &= 1 \equiv 1 \pmod{7} \\
12^1 &= 12 \equiv 5 \equiv -2 \pmod{7} \\
\to 12^1 \cdot 12^1 \equiv 5 \cdot 5 \pmod{7} \to 12^2 &\equiv 25 \equiv 4 \equiv -3 \pmod{7} \\
\to 12^1 \cdot 12^2 \equiv 5 \cdot 4 \pmod{7} \to 12^3 &\equiv 20 \equiv 6 \equiv -1 \pmod{7} \\
\to 12^1 \cdot 12^3 \equiv 5 \cdot 6 \equiv 5 \cdot (-1) \pmod{7} \to 12^4 &\equiv 30 \equiv 2 \equiv -5 \pmod{7} \\
\to 12^1 \cdot 12^4 \equiv 5 \cdot 2 \equiv 5 \cdot (-5) \pmod{7} \to 12^5 &\equiv 10 \equiv 3 \equiv -25 \equiv -4 \pmod{7} \\
\to 12^1 \cdot 12^5 \equiv 5 \cdot 3 \equiv 5 \cdot (-4) \pmod{7} \to 12^6 &\equiv 15 \equiv 1 \equiv -20 \equiv 1 \pmod{7}
\end{aligned}
$$

Los restos potenciales se repiten de 6 en 6. Fabriquemos un criterio basado en la sucesión de restos potenciales

n	0	1	2	3	4	5	6	7	8	9	...
r_n	1	5	4	6	2	3	1	5	4	6	...

así, *un primer criterio*, construido a partir del criterio general de divisibilidad, es

$$7 \mid n_{(12} \leftrightarrow 7 \mid (n_0 + 5n_1 + 4n_2 + 6n_3 + 2n_4 + 3n_5 + n_6 + 5n_7 + \ldots)$$

que enunciamos:

> un número es divisible por 7 en base 12 si, y sólo si, la cifra de las unidades más 5 veces las decenas, más 4 veces las centenas, más 6 veces las unidades de millar, más 2 veces las decenas de millar, más 3 veces las centenas de millar, más las unidades de millón, y así sucesivamente, es divisible por 7 (en base 10);

o bien en la sucesión de restos potenciales

n	0	1	2	3	4	5	6	7	8	9	...
r_n	1	5	4	−1	−5	−4	1	5	4	−1	...

así, *un segundo criterio*, construido también a partir del criterio general de divisibilidad, es

$$7 \,|\, n_{(12} \leftrightarrow 7 \,|\, (n_0 + 5n_1 + 4n_2 - n_3 - 5n_4 - 4n_5 + n_6 + 5n_7 + \ldots)$$

que enunciamos:

> un número es divisible por 7 en base 12 si, y sólo si, la cifra de las unidades más 5 veces las decenas, más 4 veces las centenas, menos las unidades de millar, menos 5 veces las decenas de millar, menos 4 veces las centenas de millar, más las unidades de millón, y así sucesivamente, es divisible por 7 (en base 10);

o bien en la sucesión de restos potenciales

n	0	1	2	3	4	5	6	7	8	9	...
r_n	1	−2	−3	−1	2	3	1	−2	−3	−1	...

así, *un tercer criterio*, construido también a partir del criterio general de divisibilidad, es

$$7 \,|\, n_{(12} \leftrightarrow 7 \,|\, (n_0 - 2n_1 - 3n_2 - n_3 + 2n_4 + 3n_5 + n_6 - 2n_7 + \ldots)$$

que enunciamos:

> un número es divisible por 7 en base 12 si, y sólo si, la cifra de las unidades menos 2 veces las decenas, menos 3 veces las centenas, menos las unidades de millar, más 2 veces las decenas de millar, más 3 veces las centenas de millar, más las unidades de millón, y así sucesivamente, es divisible por 7 (en base 10). ■

Ejemplo 573

> Demostremos que el número 79C es divisible por 7 en base 12.

Resolución.— En efecto, este hecho se sigue de la aplicación de cualquiera de los criterios propuestos en el ejemplo inmediatamente anterior:

- por el primer criterio, 79C es divisible por 7 en base 12 porque $11 + 5 \cdot 9 + 4 \cdot 7 = 84$ es divisible por 7 en base 10;
- por el segundo criterio, 79C es divisible por 7 en base 12 porque $11 + 5 \cdot 9 + 4 \cdot 7 = 84$ es divisible por 7 en base 10, y
- por el tercer criterio, 79C es divisible por 7 en base 12 porque $11 - 2 \cdot 9 - 3 \cdot 7 = -28$ es divisible por 7 en base 10. ■

Actividad 18.29

Hallemos el criterio de divisibilidad por 2 en base 10.

Actividad 18.30

Hallemos el criterio de divisibilidad por 3 en base 10.

Actividad 18.31

Hallemos el criterio de divisibilidad por 2 en base 7.

Ejemplo 574

Utilicemos el criterio general de divisibilidad en cualquier base (CGD) para hallar criterios de divisibilidad por 7, por 11 y por 13, en base diez.

[EFO 1.6.2017:4a], [EFE 22.6.2022:5a] (divisibilidad por 11), [EFE 19.1.2023:5a], [EFO 24.5.2023:5b], [EFO 27.5.2025:5b] (divisibilidad por 11), [EFE 18.6.2025:5b] (divisibilidad por 11).

Resolución.— A partir del CGD, hallemos criterios de divisibilidad por 7, por 11 y por 13, en base diez.

1. *Un criterio de divisibilidad por 7 en base diez.*

   Calculemos la sucesión de restos potenciales sucesivos de 10 módulo 7 (aplicamos: la propiedad multiplicativa de congruencias; el resultado de que al ser coprimos 10 y 7 no hay parte no periódica, y el hecho de que cuando se repite por primera vez 1, ahí comienza de nuevo la secuencia finita identificada de restos):

$$
\begin{aligned}
10^0 &\equiv 1 \pmod 7,\\
10^1 &\equiv 3 \pmod 7,\\
10^2 = 10^1 \cdot 10^1 &\equiv 3 \cdot 3 = 9 \equiv 2 \pmod 7,\\
10^3 = 10^1 \cdot 10^2 &\equiv 3 \cdot 2 = 6 \equiv -1 \pmod 7,\\
10^4 = 10^1 \cdot 10^3 &\equiv 3 \cdot (-1) = -3 \pmod 7,\\
10^5 = 10^1 \cdot 10^4 &\equiv 3 \cdot (-3) = -9 \equiv -2 \pmod 7,\\
10^6 = 10^1 \cdot 10^5 &\equiv 3 \cdot (-2) = -6 \equiv -(-1) = 1 \pmod 7.
\end{aligned}
$$

   La sucesión de restos potenciales sucesivos de 10 módulo 7, $r_0, r_1, r_2, r_3, r_4, r_5, \ldots$ es

$$1, 3, 2, -1, -3, -2, 1, 3, 2, -1, -3, -2, 1, 3, 2, \ldots,$$

por lo que por el criterio general de divisibilidad, $n = n_k \ldots n_2 n_1 n_0$ es divisible por 7 si, y sólo si, $n_0 r_0 + n_1 r_1 + n_2 r_2 + \ldots + n_k r_k$ es divisible por 7, esto es,

> $n = n_k \ldots n_2 n_1 n_0$ es divisible por 7 si, y sólo si, $n_0 + 3n_1 + 2n_2 - n_3 - 3n_4 - 2n_5$, y así sucesivamente hasta llegar a n_k, es divisible por 7;

lo enunciamos:

> en el sistema de numeración decimal, un número es divisible por 7 si, y sólo si, su cifra de las unidades más tres veces su cifra de las decenas, más dos veces su cifra de las centenas, menos su cifra de las unidades de millar, menos tres veces su cifra de las decenas de millar, menos dos veces su cifra de las centenas de millar, más su cifra de las unidades de millón, y así sucesivamente, es divisible por 7.

II. *Un criterio de divisibilidad por* 11 *en base diez.*

Calculemos la sucesión de restos potenciales sucesivos de 10 módulo 11 (aplicamos: la propiedad multiplicativa de congruencias; el resultado de que al ser coprimos 10 y 11 no hay parte no periódica, y el hecho de que cuando se repite por primera vez 1, ahí comienza de nuevo la secuencia finita identificada de restos):

$$10^0 \equiv 1 \pmod{11},$$
$$10^1 \equiv -1 \pmod{11},$$
$$10^2 = 10^1 \cdot 10^1 \equiv (-1) \cdot (-1) = 1 \pmod{11}.$$

La sucesión de restos potenciales sucesivos de 10 módulo 11, $r_0, r_1, r_2, r_3, r_4, r_5, \ldots$ es

$$1, -1, 1, -1, 1, -1, 1, \ldots,$$

por lo que por el criterio general de divisibilidad, $n = n_k \ldots n_2 n_1 n_0$ es divisible por 11 si, y sólo si, $n_0 r_0 + n_1 r_1 + n_2 r_2 + \ldots + n_k r_k$ es divisible por 11, esto es,

> $n = n_k \ldots n_2 n_1 n_0$ es divisible por 11 si, y sólo si, $n_0 - n_1 + n_2 - n_3 + n_4 - n_5$, y así sucesivamente hasta llegar a n_k, es divisible por 11;

lo enunciamos:

> en el sistema de numeración decimal, un número es divisible por 11 si, y sólo si, su cifra de las unidades menos su cifra de las decenas, más su cifra de las centenas, menos su cifra de las unidades de millar, más su cifra de las decenas de millar, menos su cifra de las centenas de millar, más su cifra de las unidades de millón, y así sucesivamente, es divisible por 11;

claro que $n_0 - n_1 + n_2 - n_3 + n_4 - n_5 + \ldots = (n_0 + n_2 + n_4 + \ldots) - (n_1 + n_3 + n_5 + \ldots)$, por lo que quizás mejor:

> en el sistema de numeración decimal, el número $n = n_k \dots n_2 n_1 n_0$ es divisible por 11 si, y sólo si, la suma de sus cifras de lugar par (comenzando por n_0, la cifra de lugar cero) menos la suma de sus cifras de lugar impar es divisible por 11;

también, leyendo directamente $n_0 - n_1 + n_2 - n_3 + n_4 - n_5 + \dots$:

> en el sistema de numeración decimal, un número es divisible por 11 si, y sólo si, la *suma alternada*[46] de sus cifras de derecha a izquierda es divisible por 11.

Por ejemplo, 123456789 es divisible por 11 si, y sólo si, $9-8+7-6+5-4+3-2+1$ es divisible por 11.

III. *Un criterio de divisibilidad por* 13 *en base diez*.

Calculemos la sucesión de restos potenciales sucesivos de 10 módulo 13 (aplicamos: la propiedad multiplicativa de congruencias; el resultado de que al ser coprimos 10 y 13 no hay parte no periódica, y el hecho de que cuando se repite por primera vez 1, ahí comienza de nuevo la secuencia finita identificada de restos):

$$\begin{aligned}
10^0 &\equiv 1 \pmod{13},\\
10^1 &\equiv -3 \pmod{13},\\
10^2 = 10^1 \cdot 10^1 &\equiv (-3)\cdot(-3) = 9 \equiv -4 \pmod{13},\\
10^3 = 10^1 \cdot 10^2 &\equiv (-3)\cdot(-4) = 12 \equiv -1 \pmod{13},\\
10^4 = 10^1 \cdot 10^3 &\equiv (-3)\cdot(-1) = 3 \pmod{13},\\
10^5 = 10^1 \cdot 10^4 &\equiv (-3)\cdot 3 = -9 \equiv -(-4) = 4 \pmod{13},\\
10^6 = 10^1 \cdot 10^5 &\equiv (-3)\cdot 4 = -12 \equiv -(-1) = 1 \pmod{13}.
\end{aligned}$$

La sucesión de restos potenciales sucesivos de 10 módulo 13, $r_0, r_1, r_2, r_3, r_4, r_5, \dots$ es

$$1, -3, -4, -1, 3, 4, 1, -3, -4, -1, 3, 4, 1, -3, -4, \dots,$$

por lo que por el criterio general de divisibilidad, $n = n_k \dots n_2 n_1 n_0$ es divisible por 13 si, y sólo si, $n_0 r_0 + n_1 r_1 + n_2 r_2 + \dots + n_k r_k$ es divisible por 13, esto es,

> $n = n_k \dots n_2 n_1 n_0$ es divisible por 13 si, y sólo si, $n_0 - 3n_1 - 4n_2 - n_3 + 3n_4 + 4n_5$, y así sucesivamente hasta llegar a n_k, es divisible por 13;

lo enunciamos:

> en el sistema de numeración decimal, un número es divisible por 13 si, y sólo si, su cifra de las unidades menos tres veces su cifra de las decenas, menos cuatro veces su cifra de las centenas, menos su cifra de las unidades de millar, más tres veces su cifra

[46] Si no se expresa nada en contra, asumimos que el término inicial de la suma alternada es positivo.

de las decenas de millar, más cuatro veces su cifra de las centenas de millar, más su cifra de las unidades de millón, y así sucesivamente, es divisible por 13. ■

Ejemplo 575

Utilicemos los criterios de divisibilidad por 7, 11 y 13 para demostrar que, en base diez, el número natural de seis cifras $abcabc$ es divisible por 1001.

[EFO 1.6.2017:4b], [EFE 19.1.2023:5b], [EFO 24.5.2023:5c].

Resolución.— Sea $n = abcabc$. Como $1001 = 7 \cdot 11 \cdot 13$, hemos de demostrar que $7 \,|\, n$, $11 \,|\, n$ y $13 \,|\, n$. Veamos. Según los criterios hallados en el apartado anterior:

$7 \,|\, n$ si, y sólo si, $(c + 3b + 2a - c - 3b - 2a) = 0$ es múltiplo de 7;

$11 \,|\, n$ si, y sólo si, $c - b + a - c + b - a) = 0$ es múltiplo de 11;

$13 \,|\, n$ si, y sólo si, $c - 3b - 4a - c + 3b + 4a) = 0$ es múltiplo de 13.

Como, ciertamente, $7 \,|\, 0$, $11 \,|\, 0$ y $13 \,|\, 0$, se tiene que $7 \,|\, n$, $11 \,|\, n$ y $13 \,|\, n$, respectivamente y, por lo tanto, que $1001 \,|\, abcabc$. ■

Ejemplo 576

Utilicemos el criterio de divisibilidad por 11 para encontrar todos los valores de a y b para los que el número decimal de tres cifras $1ab$ es divisible por 55.

[EFE 25.6.2019:4b].

Resolución.— Como $1ab$ debe ser divisible por 55, también debe serlo por 11 y por 5.

Por un lado, como debe ser divisible por 11, también debe serlo $(1+b)-a$. Como $1 \leq 1+b \leq 10$ y $-9 \leq -a \leq 0$, entonces, sumando, $-8 \leq (1 + b) + (-a) \leq 10$, y como el único múltiplo de 11 en $[-8, 10]$ es 0, se tiene que $(1 + b) - a = 0$, esto es, $1 + b = a$.

Por otro lado, como $1ab$ debe ser divisible por 5, $b = 0$ o $b = 5$, de donde $1 = a$ o $1+5 = a$, y por tanto, $1ab$ es 110 o 165 (que, en efecto, son múltiplos de 55 ya que son $55 \cdot 2$ y $55 \cdot 3$, respectivamente). ■

Ejemplo 577

Utilicemos el criterio general de divisibilidad para hallar un criterio de divisibilidad por 101 en base diez.

[EFE 22.6.2022:5b], [EFO 27.5.2025:5b] (divisibilidad por 101), [EFE 18.6.2025:5b] (divisibilidad por 101).

Resolución.— Para poder aplicar el criterio general de divisibilidad en el sistema de numeración decimal, calculemos primero los restos potenciales sucesivos de 10 módulo 101:

$$10^0 \equiv 1 \pmod{101}, \text{ esto es, } r_0 = 1,$$
$$10^1 \equiv 10 \pmod{101}, \text{ esto es, } r_1 = 10,$$
$$10^2 = 100 \equiv -1 \pmod{101}, \text{ esto es, } r_2 = -1,$$

(parece más fácil operar y recordar -1 que 100, pero es algo enteramente a nuestra elección, somos quienes «fabricamos» el criterio)

$$10^3 = 10^1 \cdot 10^2 \equiv 10 \cdot (-1) = -10 \pmod{101}, \text{ esto es, } r_3 = -10, \qquad \text{[prop. multiplicativa]}$$
$$10^4 = 10^2 \cdot 10^2 \equiv (-1) \cdot (-1) = 1 \pmod{101}, \text{ esto es, } r_4 = 1, \qquad \text{[prop. multiplicativa]}$$

esto es, $r_4 = r_0$, es decir, los restos comienzan a repetirse de forma periódica, por lo que la sucesión de restos potenciales sucesivos de 10 módulo 101, $r_0, r_1, r_2, \ldots$, es 1, 10, -1, -10, 1, 10, -1, -10, 1, 10, ...—no hay residuos en la parte no periódica porque 10 y 101 son primos entre sí—.

Aplicando ahora el criterio general de divisibilidad en base 10, $n = n_k \ldots n_2 n_1 n_0$ es divisible por 101 si, y sólo si, $n_0 r_0 + n_1 r_1 + n_2 r_2 + \ldots + n_k r_k$ es divisible por 101, esto es,

> $n = n_k \ldots n_2 n_1 n_0$ es divisible por 101 si, y sólo si, $n_0 + 10n_1 - n_2 - 10n_3 + n_4 + 10n_5 - n_6 - 10n_7$, y así sucesivamente hasta llegar a n_k, es divisible por 101;

lo enunciamos:

> en el sistema de numeración decimal, un número es divisible por 101 si, y sólo si, su cifra de las unidades más diez veces su cifra de las decenas, menos su cifra de las centenas, menos diez veces su cifra de las unidades de millar, más su cifra de las decenas de millar, más diez veces su cifra de las centenas de millar, menos su cifra de las unidades de millón, y así sucesivamente, es divisible por 101;

claro que $n_0+10n_1-n_2-10n_3+n_4+10n_5-n_6-10n_7 = n_1n_0-n_3n_2+n_5n_4-n_7n_6+n_9n_8-n_{11}n_{10}+\ldots$, por lo que también:

> en el sistema de numeración decimal, un número es divisible por 101 si, y sólo si, la suma alternada de sus cifras en bloques de dos de derecha a izquierda es divisible por 101.

Por ejemplo, 123456789 es divisible por 101 si, y sólo si, $89 - 67 + 45 - 23 + 1$ es divisible por 101. ■

Actividad 18.32

Demostremos que el número $xyxy$ es divisible por 101 y que el número $xyzxyz$ es divisible por 1001. ¿Son estos casos iniciales de una regla?

Ejemplo 578

En el sistema de numeración decimal —base 10—, determinemos las cifras x e y para que el número $7x1y4$ sea múltiplo de 11 y de 101.

[EFE 22.6.2022:5c], [EFO 27.5.2025:5c], [EFE 18.6.2025:5c].

Resolución.—

I. *Consecuencia de exigir que sea múltiplo de* 11.

Por un lado, para que $7x1y4$ sea múltiplo de 11, por el criterio de divisibilidad por 11, se deduce que debe satisfacerse que $(4+1+7)-(y+x)$ es múltiplo de 11, esto es, $12-(y+x)$ es múltiplo de 11, esto es, $-(y+x)$ es de la forma múltiplo de 11 menos 12.

El conjunto de los múltiplos de 11 es $M(11) = \{\dots, -33, -22, -11, 0, 11, 22, 33, \dots\}$, restándoles 12, $M(11) - 12 = \{\dots, -45, -34, -23, -12, -1, 10, 21, \dots\}$. Como x e y son cifras decimales, $0 \leq x, y \leq 9$, entonces $0 \leq x+y \leq 18$, de donde $-18 \leq -(x+y) \leq 0$, por lo que suceder $-(y+x) \in M(11) - 12$ significa que $-(x+y) = -1$, o que $-(x+y) = -12$, esto es, x e y satisfacen dos situaciones posibles: bien $x+y=1$, bien $x+y=12$.

II. *Consecuencia de exigir que sea múltiplo de* 101.

Por otro lado, de tener que ser $7x1y4$ múltiplo de 101, por el criterio de divisibilidad por 101, se deduce que x e y satisfacen que $4+10y-1-10x+7$ es múltiplo de 101, esto es, $10+10y-10x$ es múltiplo de 101, esto es, $10\cdot(1+y-x)$ es múltiplo de 101 y como $10\cdot(1+y-x)$ es múltiplo de 101 y 10 no es múltiplo de 101, entonces[47] $1+y-x$ es múltiplo de 101, pero como x e y son cifras decimales —base 10—, $0 \leq x, y \leq 9$, entonces $-9 \leq y-x \leq 9$ y, por tanto, $-8 \leq 1+y-x \leq 10$.

El único múltiplo de 101 en esas condiciones, esto es, entre -8 y 10, es 0, por lo que x e y satisfacen una única situación posible, a saber, $1+y-x=0$.

III. *Consecuencia de exigir que sea múltiplo de* 11 *y de* 101.

En resumen, de ser múltiplo de 11 hemos deducido dos situaciones posibles, $x+y=1$ o $x+y=12$, y de ser múltiplo de 101, una situación posible, $1+y-x=0$.

[47] Por el lema de EUCLIDES —*cfr. supra* teorema 18.37 (pág. 972 de esta edición)—, al ser $\text{mcd}(101, 10) = 1$.

Tenemos, pues, $1 \cdot 2 = 2$ situaciones combinadas posibles[48], dos sistemas de ecuaciones: $\{1 + y - x = 0, x + y = 1\}$ y $\{1 + y - x = 0, x + y = 12\}$, cuya resolución es:

$\wedge$	$x + y = 1$	$x + y = 12$
$1 + y - x = 0$	$x = 1$, $y = 0$. Solución válida.	$x = 13/2$, $y = 11/2$. Solución no válida: ni x ni y son cifras decimales.

Como vemos, hay una única solución, $x = 1$ e $y = 0$. Por lo tanto, el número buscado es 71 104.

Solución.— En el sistema de numeración decimal, las cifras x e y para las cuales el número $7x1y4$ es múltiplo de 11 y de 101, son $x = 1$ e $y = 0$. ■

Ejemplo 579

En el sistema de numeración decimal, hallemos las cifras x e y para que el número $12xy567$ sea divisible por 33.

[Cubit 134].

Resolución.— Como $33 = 3 \cdot 11$, ser divisible por 33 es serlo simultáneamente por 3 y por 11.

Un número es divisible por 3 precisamente si lo es la suma de sus cifras, en este caso,

$$3 \mid 12xy567 \leftrightarrow 3 \mid (7 + 6 + 5 + y + x + 2 + 1),$$

esto es,

$$\begin{aligned} 3 \mid 12xy567 &\leftrightarrow 3 \mid (21 + x + y) \\ &\leftrightarrow 21 + x + y = \dot{3} \\ &\leftrightarrow x + y = \dot{3} - 21. \end{aligned}$$

Además, x e y son cifras decimales por lo que $0 \leq x, y \leq 9$, de donde $0 \leq x + y \leq 18$.

Hallamos, por tanto, qué diferencias $\dot{3} - 21$ satisfacen pertenecer a $[0, 18]$; tales diferencias son:

$$\begin{aligned} &0\ (= 3 \cdot 7 - 21), \\ &3\ (= 3 \cdot 8 - 21), \\ &6\ (= 3 \cdot 9 - 21), \end{aligned}$$

[48] *Vid. infra* el principio de la multiplicación —§ 19.1.1 (pág. 1138 de esta edición)—.

$$9\ (=3\cdot 10-21),$$
$$12\ (=3\cdot 11-21),$$
$$15\ (=3\cdot 12-21),$$
$$18\ (=3\cdot 13-21),$$

por lo que pueden suceder siete situaciones posibles, a saber, $x+y=0 \veebar x+y=3 \veebar x+y=6 \veebar x+y=9 \veebar x+y=12 \veebar x+y=15 \veebar x+y=18$.

Un número es divisible por 11 precisamente si la suma de las cifras de lugar par menos la suma de las cifras de lugar impar es divisible entre 11, en este caso,

$11|12xy567 \leftrightarrow 11|((7+5+x+1)-(6+y+2))$ esto es,

$$\begin{aligned} 11|12xy567 &\leftrightarrow 11|(5+x-y) \\ &\leftrightarrow 5+x-y=\dot{11} \\ &\leftrightarrow x-y=\dot{11}-5. \end{aligned}$$

Además, x e y son cifras decimales, por lo que $0\le x,y\le 9$, de donde $-9\le x-y\le 9$.

Hallamos, por tanto, qué diferencias $\dot{11}-5$ satisfacen pertenecer a $[-9,9]$: $\dot{11}-5 = \{\dots,-5(=0-5),6(=11-5),\dots\}$, por lo que pueden suceder dos situaciones posibles: $x-y=-5 \veebar x-y=6$.

Tenemos entonces, por el principio de la multiplicación[49], $7\cdot 2=14$ situaciones posibles:

$\wedge$	$x+y=0$	$x+y=3$	$x+y=6$	$x+y=9$	$x+y=12$	$x+y=15$	$x+y=18$
$x-y=-5$	$x=-5/2$, SNV (x NCD)	$x=-1$, SNV (x NCD)	$x=1/2$, SNV (x NCD)	$x=2$, $y=7$ SV (x,y CD)	$x=7/2$, SNV (x NCD)	$x=5$, $y=10$ SNV (x NCD)	$x=13/2$ SNV (x NCD)
$x-y=6$	$x=3$, $y=-3$ SNV (y NCD)	$x=9/2$, SNV (x NCD)	$x=6$, $y=0$ SV (x,y CD)	$x=15/2$, SNV (x NCD)	$x=9$, $y=3$ SV (x,y CD)	$x=21/2$, SNV (x NCD)	$x=12$ SNV (x NCD)

SNV: solución no válida; SV: solución válida; NCD: no es/son cifra/s decimal/es; CD: sí es/son cifra/s decimal/es.

Luego hay tres posibles soluciones: $\langle x,y\rangle \in \{\langle 2,7\rangle,\langle 6,0\rangle,\langle 9,3\rangle\}$.

Así, los números posibles son 1 227 567, 1 260 567 y 1 293 567, divisibles entre 33, siendo sus cocientes respectivos: 37 199, 38 199 y 39 199. ■

[49] *Cfr. infra* § 19.1.1 (pág. 1138 de esta edición).

Observación 18.14.3.— Existen otros criterios de divisibilidad que no surgen directamente del criterio general de divisibilidad; a modo de ejemplo, otros criterios para 7 y 11 son[50]:

- un número es divisible por 7 si, y sólo si,
  - la suma de cinco veces la última cifra y el resto es divisible por 7 (por ejemplo, 161, pues $16 + (1 \cdot 5) = 21 = 3 \cdot 7$);
  - la suma alternada en bloques de tres cifras de derecha a izquierda es divisible por 7 (por ejemplo, 108 175 616 801, pues $801 - 616 + 175 - 108 = 252 = 36 \cdot 7$);
  - la resta de dos veces la última cifra del resto es divisible por 7 (por ejemplo, 161, pues $16 - (1 \cdot 2) = 14 = 2 \cdot 7$);

  [TT], [EFEC 29.1.2025:7] (tipo test).

- un número es divisible por 11 si, y sólo si,
  - la suma en bloques de dos cifras de derecha a izquierda es divisible por 11 (por ejemplo, 253, pues $2 + 53 = 55 = 5 \cdot 11$);
  - la resta de la última cifra del resto es divisible por 11 (por ejemplo, 253, pues $25-3 = 22 = 2 \cdot 11$);
  - la suma de diez veces la última cifra y el resto es divisible por 11 (por ejemplo, 253, pues $25 + 30 = 55 = 5 \cdot 11$).

  [TT], [EFE 3.7.2024:7] (tipo test).

Actividad 18.33

De los siguientes criterios de divisibilidad por 8 en el sistema de numeración decimal, ¿cuál surge directamente del criterio general de divisibilidad? Un número es divisible por 8 si, y sólo si,

a. la suma de la cifra de las unidades más el doble de la cifra de las decenas más el cuádruple de la cifra de las centenas es divisible por 8 (por ejemplo, 262 144, pues $4 + 2 \cdot 4 + 4 \cdot 1 = 16 = 2 \cdot 8$);

b. la suma de la última cifra más el doble del resto es divisible por 8 (por ejemplo, 256, pues $6 + 2 \cdot 25 = 56 = 7 \cdot 8$);

c. el número formado por las tres últimas cifras es divisible por 8 (por ejemplo, 1152, pues $152 = 19 \cdot 8$);

d. si la cifra de las centenas es par, el número formado por las dos últimas cifras es divisible por 8 y si la cifra de las centenas es impar, el número formado por las dos últimas cifras es el cuádruple de un número impar (por ejemplo, 256, pues $56 = 7 \cdot 8$, y 1152, pues $52 = 4 \cdot 13$).

[TT], [EFE 29.1.2025:7] (tipo test).

[50] *Vid. v. gr.* https://en.wikipedia.org/wiki/Divisibility_rule.

§ 18.15 Ecuaciones diofánticas

Definición 18.35.— Llamamos *ecuación diofántica* a toda ecuación algebraica con coeficientes enteros y cuyas soluciones las busquemos en los enteros.

Teorema 18.106 (Resolución de $ax = c$)
La ecuación diofántica lineal monádica $ax = c$ tiene solución en $\mathbb{Z}$ si, y sólo si, a divide a c, y la solución es

$$x = \frac{c}{a}.$$

Teorema 18.107 (Resolución de $ax + by = c$)
La ecuación diofántica lineal diádica —en dos variables— de grado uno, $ax + by = c$, tiene soluciones en $\mathbb{Z}$ si, y sólo si, d divide a c, siendo $d = \text{mcd}(a, b)$, y la *solución general* de $ax + by = c$ es

$$\{\langle x, y\rangle : k \in \mathbb{Z}\},$$

con

$$x = x_0 + \frac{b}{d} \cdot k,$$
$$y = y_0 - \frac{a}{d} \cdot k,$$

donde $\langle x_0, y_0\rangle$, con

$$x_0 = \frac{c}{d} \cdot s,$$
$$y_0 = \frac{c}{d} \cdot t,$$

es una *solución particular* de $ax + by = c$, siendo s y t los coeficientes de BÉZOUT.

Teorema 18.108 (Resolución de $a_0x_0 + a_1x_1 + \cdots + a_nx_n = c$)
La ecuación diofántica lineal poliádica de grado uno, $a_0x_0 + a_1x_1 + \cdots + a_nx_n = c$, tiene soluciones en $\mathbb{Z}$ si, y sólo si, d divide a c, siendo $d = \text{mcd}(a_0, a_1, \ldots, a_n)$. Esta ecuación se resuelve reduciéndola a otra con una variable menos y así hasta una ecuación diádica, esto es, con sólo dos variables.

Teorema 18.109 (Resolución de $x^2 - y^2 = c$)
La ecuación diofántica no lineal diádica de grado dos, $x^2 - y^2 = c$, con $c \in \mathbb{Z}$, tiene soluciones en $\mathbb{Z}$ si, y sólo si, c admite descomposición en factores con la misma paridad (ambos pares o ambos impares).

Demostración.— Observemos, por cierto, que si puede factorizarse c en dos factores pares, c debe ser múltiplo de 4. La demostración del teorema se sigue de ser $x^2 - y^2 = (x+y)(x-y)$ y suceder que si $x + y = a$ y $x - y = b$, entonces $\langle x, y\rangle$, con $x = (a+b)/2$ e $y = (a-b)/2$, constituye una solución, porque, entonces, tanto si c es impar como si c es múltiplo de 4, cada una de tales descomposiciones con la misma paridad proporciona dos soluciones enteras $\langle x, y\rangle$, a saber,

$$\left\langle \frac{a+b}{2}, \frac{a-b}{2} \right\rangle \text{ y } \left\langle -\frac{a+b}{2}, -\frac{a-b}{2} \right\rangle,$$

mientras que si c es par pero no es múltiplo de 4, la ecuación no tiene soluciones enteras. ■

Para resolver las cuestiones de los ejemplos y actividades relativas a ecuaciones diofánticas debemos: I, proponer, razonando su porqué, una ecuación diofántica que modelice la situación expuesta, y II, demostrar que tiene al menos una solución; después, debemos utilizar los coeficientes de BÉZOUT y la teoría de las ecuaciones diofánticas para: III, calcular una solución particular de la ecuación propuesta en I; IV, calcular la solución general de la ecuación propuesta en I; V, calcular la solución de la cuestión en estudio.

Si no recordásemos cómo calcular los coeficientes de BÉZOUT o la teoría de las ecuaciones diofánticas, pudiésemos resolver los apartados III, IV y V, por teoría de congruencias.

Ejemplo 580

Imaginemos que debemos realizar un pago de 38 euros a una persona, pero en vez de euros sólo tenemos *eslagnas* (una eslagna equivale a ocho euros) y la otra persona sólo tiene *dobeles* (un dobel equivale a dos euros). Calculemos las eslagnas que debemos entregar para realizar el pago y los dobeles que deben devolvernos, siendo el número de eslagnas el menor posible.

[EPF 14.5.2019:3].

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Si x e y representan el número de eslagnas y el de dobeles, respectivamente, entonces la ecuación diofántica que representa la situación es

$$8x - 2y = 38,$$

que simplificada queda

$$4x - y = 19,$$

Tenemos así una ecuación diofántica con dos variables; estudiémosla:

II. *Demostración de que tiene al menos una solución.*

¿Tiene solución entera? Sí, por el teorema 18.107 (pág. 1047 de esta edición), pues $\operatorname{mcd}(4,-1) = \operatorname{mcd}(4,1) = 1 | 19$.

III. *Cálculo de una solución particular.*

Coeficientes de BÉZOUT: por ensayo y error, $s = 0$ y $t = -1$ (en efecto, $0 \cdot 4 + (-1) \cdot (-1) = 1$).

Así, una solución particular es:

$$x_0 = \frac{19 \cdot 0}{1} = 0,$$
$$y_0 = \frac{19 \cdot (-1)}{1} = -19.$$

Comprobación.— En efecto, $4 \cdot 0 - (-19) = 19$.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general es:

$$\begin{aligned} x &= 0 + \frac{k}{1} \cdot (-1) \\ &= -k, \\ y &= -19 + \frac{k}{1} \cdot (-4) \\ &= -19 - 4k, \end{aligned}$$

siendo $k \in \mathbb{Z}$.

Comprobación.— En efecto, $4 \cdot (-k) - (-19 - 4k) = -4k + 19 + 4k = 19$.

V. *Cálculo de la solución de la cuestión en estudio.*

Encontremos finalmente la solución particular para la cuestión en estudio. Para ello, intentemos acotar k. Comparando los cambios de moneda y la cantidad a pagar, tenemos la seguridad de que en el pago van a intervenir eslagnas y dobeles, esto es: $x > 0$ e $y > 0$ y así:

$$\begin{aligned} 0 < x &\to 0 < -k \\ &\to k < 0, \\ 0 < y &\to 0 < -19 - 4k \\ &\to 19 < -4k \\ &\to k < \frac{-19}{4} \\ &\to k \in \{\ldots, -7, -6, -5\}, \end{aligned}$$

Para que el número de eslagnas sea el menor posible, k debe ser el mayor posible, por tanto, $k = -5$, de donde $x = -(-5) = 5$ e $y = -19 - 4(-5) = 1$.

Solución.— Para realizar el pago de 38 euros con el menor número de eslagnas posible, debemos entregar 5 eslagnas (cantidad equivalente a 40 euros) y nos devolverán 1 dobel (lo que equivale a 2 euros). ■

Ejemplo 581

¿Cuáles son los números enteros positivos, múltiplos de tres, terminados en cinco y menores que cien?

[EFE 7.7.2021:6], [SEP 12.5.2022:6], [EFE 29.1.2025:9] (tipo test). *Cfr.* García, Hernández y Nevot [150]: problema propuesto (y resuelto) 1.17 (págs. 41 y 52).

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Los múltiplos de 3 son de la forma $3x$; que terminen en 5 significa que al dividir entre 10, el resto es 5, por el algoritmo de la división, existe un único y tal que

$$3x = 10y + 5,$$

es decir, tal que

$$3x + (-10)y = 5. \tag{18.37}$$

Así, x e y designan números enteros positivos (x por ser $3x$ un múltiplo positivo de 3 e y por ser el cociente de la división euclidea de $3x$ por 10).

II. *Demostración de que tiene al menos una solución.*

Como $\operatorname{mcd}(3, -10) = 1$ es un divisor de 5, entonces, por el teorema 18.107 (pág. 1047 de esta edición), esta ecuación tiene al menos una solución $\langle x, y \rangle$ con $x, y \in \mathbb{Z}$.

III. *Cálculo de una solución particular.*

Una solución particular de (18.37) es $x_0 = 5s/1$, $y_0 = 5t/1$, siendo s y t los coeficientes de Bézout de 3 y -10, coeficientes de los que sabemos que existen en número infinito; por simple inspección, escogemos $s = -3$, $t = -1$, por lo que una solución particular de (18.37) es $\langle x_0, y_0 \rangle = \langle -15, -5 \rangle$.

Comprobación.— En efecto, $3 \cdot (-15) + (-10) \cdot (-5) = 5$.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general de (18.37) es

$$\begin{cases} x = -15 + \dfrac{-10}{1}k \\ y = -5 + \dfrac{-3}{1}k \end{cases}$$

con $k \in \mathbb{Z}$.

Comprobación.— En efecto, $3 \cdot (-15 - 10k) + (-10) \cdot (-5 - 3k) = -45 - 30k + 50 + 30k = 5$.

v. *Cálculo de la solución de la cuestión en estudio*.

Para encontrar la solución de la cuestión en estudio, veamos primero qué valores son posibles para k. Las restricciones que imponen la cuestión en estudio es que x e y designan números enteros positivos y que $3x < 100$. De la solución general tenemos, por tanto, que:

$$\begin{aligned} 0 < x &\leftrightarrow 0 < -15 - 10k \\ &\leftrightarrow 15 < -10k \\ &\leftrightarrow k < -\frac{15}{10} \\ &\leftrightarrow k < -\frac{3}{2} \end{aligned}$$

y que

$$\begin{aligned} 0 < y &\leftrightarrow 0 < -5 - 3k \\ &\leftrightarrow 5 < -3k \\ &\leftrightarrow k < -\frac{5}{3} \end{aligned}$$

de donde $k < \text{mín}\left\{-\frac{5}{3}, -\frac{3}{2}\right\} = -\frac{5}{3}$.

Por otro lado,

$$\begin{aligned} 3x < 100 &\leftrightarrow 3(-15 - 10k) < 100 \\ &\leftrightarrow -45 - 30k < 100 \\ &\leftrightarrow -30k < 100 + 45 \\ &\leftrightarrow k > -\frac{145}{30} \\ &\leftrightarrow k > -\frac{29}{6} \end{aligned}$$

En definitiva,

$$-\frac{29}{6} < k < -\frac{5}{3}$$

de donde $k \in \{-4, -3, -2\}$.

Recorremos estos valores de k hallando los correspondientes valores de $x = -15 - 10k$ y de $3x$:

$$k = -4 \to \langle x, 3x \rangle = \langle 25, 75 \rangle;$$
$$k = -3 \to \langle x, 3x \rangle = \langle 15, 45 \rangle;$$
$$k = -2 \to \langle x, 3x \rangle = \langle 5, 15 \rangle.$$

Solución.— Los números enteros positivos, múltiplos de tres, terminados en cinco y menores que cien, son tres, a saber, 15, 45 y 75. ■

Observación 18.15.0.— Saber que el producto de un número impar por 5 termina en 5 —ya que $(2y+1)\cdot 5 = 10y+5$ y $10y$ termina en 0—, nos permite plantear la ecuación diofántica en el apartado 1, como igualando dicho producto, $(2y+1)\cdot 5$, a ser múltiplo de 3, esto es, a $3x$, en definitiva, $(2y+1)\cdot 5 = 3x$.

Observación 18.15.1.— El lado derecho de la ecuación $3x = 10y + 5$ sujeta a las restricciones $30x < 100$ y $0 < y \leq 9$ no es más que el desarrollo en potencias $10^1 \cdot y + 10^0 \cdot 5$ del número decimal de dos cifras $y5$.

Ejemplo 582

Se quiere empaquetar 64 objetos para su transporte. Se dispone de 5 cajas con capacidad para 8 objetos cada una y otras 5 con capacidad doble, esto es, para 16 objetos cada una. Si no se tiene por qué utilizar todas las cajas sino maximizar el número de objetos por caja, halle de cuántas formas se puede hacer el empaquetado final y cuáles son precisamente dichas formas.

[AIC 10.4.2019:6], [EFE 19.1.2023:6], [EFO 24.5.2023:6], [EFE 3.7.2024:9] (tipo test).

Resolución.— Si x e y representan el número de cajas con capacidad para 8 y 16 objetos, respectivamente, entonces tenemos lo que sigue.

1. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta*.

   Lo expuesto en el enunciado queda representado por la ecuación

   $$8x + 16y = 64,$$

   que simplificada queda

   $$x + 2y = 8.$$

   Como buscamos soluciones enteras, tenemos así una ecuación diofántica con dos variables. Esta ecuación es irreducible en los enteros debido a que los números 1, 2 y 8 son primos entre sí.

II. *Demostración de que tiene al menos una solución.*

¿Tiene solución entera? Sí, por el teorema 18.107 (pág. 1047 de esta edición), pues $\text{mcd}(1, 2) = 1$ que es divisible por 8.

III. *Cálculo de una solución particular.*

Coeficientes de BÉZOUT, existen infinitos, ya que cualquier par (p, q) con $p = 1 - 2q$ con $q \in \mathbb{Z}$ es solución de la ecuación $p + 2q = 1$. Tomamos, por ejemplo, $p = -1$ y $q = 1$.
Una solución particular es

$$x_0 = \frac{8 \cdot (-1)}{1} = -8,$$
$$y_0 = \frac{8 \cdot 1}{1} = 8.$$

Comprobación.— En efecto, $-8 + 2 \cdot 8 = 8$.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general es

$$\begin{aligned} x &= -8 + \frac{k}{1} \cdot 2 \\ &= -8 + 2k, \\ y &= 8 + \frac{k}{1} \cdot (-1) \\ &= 8 - k, \end{aligned}$$

siendo $k \in \mathbb{Z}$.

Comprobación. En efecto, $(-8 + 2k) + 2 \cdot (8 - k) = -8 + 2k + 16 - 2k = 8$.

V. *Cálculo de la solución de la cuestión en estudio.*

Encontremos finalmente la solución particular para la cuestión en estudio. Para ello, intentemos acotar k. Como nos dicen que disponemos de 5 cajas de cada tipo, tenemos: $0 \leq x \leq 5$ y $0 \leq$

$y \leq 5$ (x e y son enteros no negativos porque representan números de cajas) y así:

$$\begin{aligned} 0 \leq x \leq 5 &\to 0 \leq -8 + 2k \leq 5 \\ &\to 8 \leq 2k \leq 13 \\ &\to 4 \leq k \leq 6 + \frac{1}{2} \\ &\to k \in \{4, 5, 6\}, \\ 0 \leq y \leq 5 &\to 0 \leq 8 - k \leq 5 \\ &\to -8 \leq -k \leq -3 \\ &\to 3 \leq k \leq 8 \\ &\to k \in \{3, 4, 5, 6, 7, 8\}, \end{aligned}$$

de donde:

$$(4 \leq k \leq 6) \wedge k \in \mathbb{Z}.$$

Se tienen entonces los siguientes valores para x, y, z según los valores de k:

$k =$	4	5	6
$x = -8 + 2k =$	0	2	4
$y = 8 - k =$	4	3	2

Solución.—Como en ningún momento nos dicen que tengamos que utilizar cajas de ambos tipos, se tiene que existen tres formas de hacer el empaquetado final y son: $(x, y) = (0, 4)$, $(x, y) = (2, 3)$ y $(x, y) = (4, 2)$, esto es:

a. una primera forma en la que se usan 0 cajas con capacidad de 8 y 4 con capacidad de 16 (con un total de $0 + 64$ objetos);

b. una segunda forma en la que se usan 2 cajas con capacidad de 8 y 3 con capacidad de 16 (con un total de $16 + 48$ objetos), y

c. una tercera forma en la que se usan 4 cajas con capacidad para 8 objetos y 2 con capacidad de 16 (un total de $32 + 32$ objetos).

Todas estas formas priorizan maximizar el número de objetos por caja. ■

Observación 18.15.2.— En III, $(-8, 8)$ es una solución particular de $x + 2y = 8$; no debe extrañarnos que $-8 < 0$ ni que $5 < 8$ pues, en ese momento, aún no hemos introducido ninguna restricción.

Ejemplo 583

Una distribuidora hizo un pedido indefinido de un superventas a una editorial, solicitó «entre 7000 y 8000 ejemplares». La editorial se los envió en embalajes con 70 ejemplares cada uno. La distribuidora los repartió a las librerías en cajas con 23 ejemplares cada una, quedando en existencia (sin repartir) 33 ejemplares. ¿Cuál fue el número de ejemplares que la editorial envió a la distribuidora?

[EFO 17.1.2022:6], [PEP 5.4.2022:6], [EFO 20.5.2022:6]. *Cfr.* García, Hernández y Nevot [150]: problema de recapitulación 1.1 (pág. 42).

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Si n es el número de ejemplares que la editorial envió a la distribuidora en x embalajes e y es el número de cajas que repartió la distribuidora a las librerías, entonces lo expuesto en el enunciado se formaliza como

$$n = 70x \qquad (18.38)$$
$$n = 23y + 33$$

sujeto a la restricción de que $7000 \leq n \leq 8000$.

Tenemos, pues, que $70x = 23y + 33$ y en definitiva que resolver la ecuación diofántica

$$70x + (-23)y = 33.$$

II. *Demostración de que tiene al menos una solución.*

Por lo establecido en el teorema 18.107 (pág. 1047 de esta edición), esta ecuación tiene solución entera, ya que $\operatorname{mcd}(70, -23) = 1$; en efecto, calculamos el $\operatorname{mcd}(70, 23)$ —que es igual al de 70 y -23— por el algoritmo de Euclides,

$$70 = 3 \cdot 23 + 1, \qquad (18.39)$$
$$23 = 23 \cdot 1 + 0,$$

viendo que el resto anterior al nulo vale 1.

III. *Cálculo de una solución particular.*

De (18.39),

$$1 \cdot 70 + 3 \cdot (-23) = 1,$$

por lo que los coeficientes de BÉZOUT s y t son 1 y 3, respectivamente, esto es, una solución —particular— de $70x + (-23)y = 1$ es $\langle x, y\rangle = \langle 1, 3\rangle$.

Una solución —particular— de $70x + (-23)y = 33$ es

$$x_0 = \frac{1 \cdot 33}{1},$$
$$y_0 = \frac{3 \cdot 33}{1}.$$

Comprobación.— En efecto, $70 \cdot 33 + (-23) \cdot 99 = 33$.

IV. *Cálculo de la solución general a partir de la particular anterior*.

La solución general —o sea, todas las soluciones— de $70x + (-23)y = 33$, tomando como solución particular la anterior, es

$$x = 1 \cdot 33 + k \cdot \frac{(-23)}{1},$$
$$y = 3 \cdot 33 - k \cdot \frac{70}{1}\ (k \in \mathbb{Z}),$$

esto es,

$$x = 33 - 23k, \tag{18.40}$$
$$y = 99 - 70k\ (k \in \mathbb{Z}).$$

Comprobación.— En efecto, $70\cdot(33-23k)+(-23)\cdot(99-70k) = 2310-1610k-2277+1610k = 33$.

V. *Cálculo de la solución de la cuestión en estudio*.

Calculemos, finalmente, la solución de la cuestión en estudio.

$$\begin{aligned}
77000 \leq n \leq 8000 &\leftrightarrow 7000 \leq 70x \leq 8000 && \text{[por (18.38)]}\\
&\leftrightarrow 700 \leq 7x \leq 800 && \text{[dividiendo por 10]}\\
&\leftrightarrow 700 \leq 7\cdot(33-23k) \leq 800 && \text{[sustitución por (18.40)]}\\
&\leftrightarrow 700 \leq 231 - 161k \leq 800 && [\text{aritmética en } (\mathbb{Z}, +, \cdot, \leq)]\\
&\leftrightarrow 700 - 231 \leq -161k \leq 800 - 231 && [\text{aritmética en } (\mathbb{Z}, +, \cdot, \leq)]\\
&\leftrightarrow 469 \leq -161k \leq 569 && [\text{aritmética en } (\mathbb{Z}, +, \cdot, \leq)]\\
&\leftrightarrow 2,913 \leq -k \leq 3,534 && [\text{aritmética en } (\mathbb{Z}, +, \cdot, \leq)]\\
&\leftrightarrow -3,534 \leq k \leq -2,913 && [\text{aritmética en } (\mathbb{Z}, +, \cdot, \leq)],
\end{aligned}$$

luego, como $k \in \mathbb{Z}$, $k = -3$, por lo que $x = 33 - 23 \cdot (-3) = 102$ y, por tanto, $n = 70 \cdot 102 = 7140$.

Solución.— La editorial envió a la librería 7140 ejemplares. ■

Ejemplo 584

Se sabe que un texto sólo tiene palabras de una, dos o tres letras; entonces, si el texto tuviese 11 letras y constase de 6 palabras, ¿cuántas palabras de cada tipo tendría?

[EFO 4.6.2021:6], [EFEC 29.1.2025:9] (tipo test).

Resolución.— Representemos por x, y, z los números de palabras de una, dos y tres letras, respectivamente. Con esta representación los totales de letras de palabras de cada tipo, esto es, de una, dos y tres letras, son x, $2y$ y $3z$, respectivamente.

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta*.

Por una parte, como el texto consta de 6 palabras, la suma de los números de palabras de cada tipo x, y, z, es 6, esto es, $x + y + z = 6$ (subyace el principio de la adició[51]n [¡esto requiere justificación! ✍]); por la otra, como hay 11 letras, la suma de las letras respectivas es 11, es decir, $x + 2y + 3z = 11$ (subyace el principio de la adición y en cada sumando el de la multiplicación[52] [¡esto requiere justificación! ✍]). Si restamos la primera ecuación de la segunda, obtenemos la *ecuación diofántica*

$$y + 2z = 5. \tag{18.41}$$

II. *Demostración de que (18.41) tiene al menos una solución*.

Como $\operatorname{mcd}(1, 2) = 1$ es un divisor de 5, entonces, por el teorema 18.107 (pág. 1047 de esta edición), *esta ecuación tiene al menos una solución* (y, z) con $y, z \in \mathbb{Z}$.

III. *Cálculo de una solución particular*.

Una solución particular de (18.41) es $y_0 = 5s/1$, $z_0 = 5t/1$, siendo s y t los coeficientes de BÉZOUT de 1 y 2, coeficientes de los que sabemos que existen en número infinito; por simple inspección, escogemos $s = -1$, $t = 1$, por lo que *una solución particular* de (18.41) es $(y_0, z_0) = (-5, 5)$.

Comprobación.— En efecto, $-5 + 2 \cdot 5 = 5$.

IV. *Cálculo de la solución general a partir de la particular anterior*.

[51] *Vid. infra* § 19.1.0 (pág. 1136).
[52] *Vid. infra* § 19.1.1 (pág. 1138).

La solución general de (18.41) es

$$\begin{cases} y = -5 + \frac{2}{1}k \\ z = 5 + \frac{-1}{1}k \end{cases}$$

con $k \in \mathbb{Z}$.

Comprobación.— En efecto, $(-5 + 2k) + 2 \cdot (5 - k) = -5 + 2k + 10 - 2k = 5$.

v. *Cálculo de la solución de la cuestión en estudio*.

Para encontrar *la solución de la cuestión en estudio*, veamos primero qué valores son posibles para k. La única restricción que impone la cuestión en estudio es que como x, y, z designan números de palabras, deben tener valores no negativos. De la solución general tenemos, por tanto, que:

$$\begin{aligned} 0 \leq y &\leftrightarrow 0 \leq -5 + 2k \\ &\leftrightarrow 5 \leq 2k \\ &\leftrightarrow \frac{5}{2} \leq k \end{aligned}$$

y que

$$\begin{aligned} 0 \leq z &\leftrightarrow 0 \leq 5 - k \\ &\leftrightarrow k \leq 5, \end{aligned}$$

de donde $k \in \{3, 4, 5\}$. Recorremos estos valores de k hallando los correspondientes valores de $y = -5 + 2k$, $z = 5 - k$ y $x = 6 - y - z$:

$$\begin{aligned} k = 3 &\rightarrow \langle x, y, z \rangle = \langle 3, 1, 2 \rangle; \\ k = 4 &\rightarrow \langle x, y, z \rangle = \langle 2, 3, 1 \rangle; \\ k = 5 &\rightarrow \langle x, y, z \rangle = \langle 1, 5, 0 \rangle. \end{aligned}$$

Solución.— Si el texto constase de 6 palabras y 11 letras, podrían darse tres situaciones:

0.ª que el texto conste de 1 palabra de una letra y 5 de dos letras;

1.ª que el texto conste de 2 palabras de una letra, 3 de dos letras y 1 de tres letras, o

2.ª que el texto conste de 3 palabras de una letra, 1 de dos letras y 2 de tres letras. ■

Actividad 18.34

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición y el principio de la multiplicación, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Ejemplo 585

¿Qué número natural n es aquél para el que la suma de sus cifras es 20 y tal que el número $(n-205)/2$ tiene las mismas cifras que n escritas en orden inverso?

[EFE 22.6.2022:6]. *Cfr.* ANZOLA y CARUNCHO [197]: ejercicio 8.1 (pág. 181).

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

0. *Traducción de los requerimientos.*

El número n no puede tener dos cifras porque la suma máxima sería 18 y no 20. Como hay que restar 205, lo más simple es suponer que el número tiene tres cifras; supongamos, pues, que $n = n_2 n_1 n_0$, con $0 \leq n_i \leq 9$—también deducimos del enunciado que $n \geq 205$, por si sirviese para algo—.

Traduzcamos los requerimientos:

0.º, «la suma de sus cifras es 20»: $n_2 + n_1 + n_0 = 20$;

1.º, «el número $(n-205)/2$»: $\dfrac{100n_2 + 10n_1 + n_0 - 205}{2}$, ya que $100n_2 + 10n_1 + n_0$ es la representación decimal de $n = n_2 n_1 n_0$;

2.º, «las mismas cifras que n escritas en orden inverso»: $100n_0 + 10n_1 + n_2$.

Así, según el enunciado, las cifras buscadas deben ser la solución del sistema:

$$n_2 + n_1 + n_0 = 20$$
$$\frac{100n_2 + 10n_1 + n_0 - 205}{2} = 100n_0 + 10n_1 + n_2$$

1. *Propuesta de una ecuación diofántica.*

Conocemos un método para solucionar ecuaciones diofánticas del tipo $ax + by = c$; así que habría que conseguir llegar a una ecuación con esta forma—,

esto es, las cifras buscadas son la solución del sistema de ecuaciones diofánticas:

$$n_2 + n_1 + n_0 = 20$$
$$98n_2 - 10n_1 - 199n_0 = 205,$$

sistema que simplificamos multiplicando la primera ecuación por 10 y sumándola a la segunda para obtener así la ecuación diofántica lineal en dos variables

$$108n_2 - 189n_0 = 405,$$

que es de la forma buscada.

Como $108 = 2^2 \cdot 3^3$, $189 = 3^3 \cdot 7$ y $405 = 3^3 \cdot 3 \cdot 5$, $\operatorname{mcd}(108, 189, 405) = 3^3 = 27$, y esta ecuación se simplifica en

$$4n_2 - 7n_0 = 15,$$

en la que, por comodidad para comparar con el teorema 18.107 (pág. 1047 de esta edición), notamos n_2 por x y n_0 por y, de manera que esta ecuación, en formato $ax + by = c$, es

$$4x + (-7)y = 15. \tag{18.42}$$

II. *Demostración de que tiene al menos una solución*.

Por lo establecido en el teorema 18.107 (pág. 1047 de esta edición), esta ecuación tiene solución en $\mathbb{Z}$ si, y sólo si, $d = \operatorname{mcd}(4, -7)$ divide a 15, lo que sucede, pues, por un lado, $d = \operatorname{mcd}(4, -7) = \operatorname{mcd}(|4|, |-7|) = 1$—en efecto, por el algoritmo de Euclides,

$$7 = 4 \cdot 1 + 3,$$
$$4 = 3 \cdot 1 + 1,$$
$$3 = 1 \cdot 3 + 0,$$

por lo que $d = \operatorname{mcd}(7, 4) = 1$ (último resto no nulo)—; por otro, $1 \mid 15$; así que la ecuación tiene solución entera.

III. *Una solución particular* de $4x + (-7)y = 15$ es

$$x_0 = \frac{15}{1} \cdot s,$$
$$y_0 = \frac{15}{1} \cdot t,$$

donde s y t son los coeficientes de Bézout de 4 y -7—esto es, los coeficientes de la expresión del máximo común divisor como combinación lineal de 4 y -7, $s4 + t(-7) = 1$—. Es posible hallar estos coeficientes utilizando el algoritmo de Euclides extendido, o bien de la siguiente manera. Como por el algoritmo de Euclides —*vid.* el párrafo anterior—, $4 = 3 \cdot 1 + 1$, entonces

$$1 = 4 - 3 \cdot 1; \tag{18.43}$$

como $7 = 4 \cdot 1 + 3$—por el algoritmo de Euclides, ejecutado en el párrafo anterior—, entonces

$$3 = 7 - 4 \cdot 1; \tag{18.44}$$

ahora, sustituyendo (18.44) en (18.43), se tiene que

$$\begin{aligned}1 &= 4 - (7 - 4 \cdot 1) \cdot 1, \text{ entonces}\\ 1 &= 4 \cdot 1 + 4 \cdot 1 - 7 \cdot 1, \text{ de donde}\\ 1 &= 4 \cdot (1 + 1) - 7 \cdot 1, \text{ por lo que}\\ 1 &= 4 \cdot 2 - 7 \cdot 1, \text{ esto es,}\\ 1 &= 2 \cdot 4 + 1 \cdot (-7),\end{aligned}$$

de donde $s = 2$ y $t = 1$ —los coeficientes de Bézout de 4 y -7—, y entonces, una solución particular de $4x + (-7)y = 15$ es

$$\begin{aligned}\langle x_0, y_0 \rangle &= \left\langle \frac{15}{1} \cdot 2, \frac{15}{1} \cdot 1 \right\rangle\\ &= \langle 30, 15 \rangle.\end{aligned}$$

Comprobación.— En efecto, $4 \cdot 30 + (-7) \cdot 15 = 120 - 105 = 15$.

IV. *Cálculo de la solución general a partir de la particular anterior*.

La solución general de $4x + (-7)y = 15$ es

$$\begin{aligned}x &= 30 + k \cdot (-7),\\ y &= 15 + k \cdot (-4),\end{aligned}$$

con $k \in \mathbb{Z}$.

Comprobación.— En efecto, $4 \cdot (30 - 7k) + (-7) \cdot (15 - 4k) = 120 - 28k - 105 + 28k = 15$.

V. *Cálculo de la solución de la cuestión en estudio*.

Para encontrar la solución concreta de la cuestión en estudio, estudiemos primero qué valores son posibles para k.

Por una parte, de la solución general, tenemos $x = 30 - 7k$, con $0 \leq x \leq 9$ —x es una cifra decimal—, esto es,

$$\begin{aligned}0 \leq 30 - 7k \leq 9 &\to -30 \leq -7k \leq -30 + 9\\ &\to 30 - 9 \leq 7k \leq 30\\ &\to 21/7 \leq k \leq 30/7\\ &\to 3 \leq k \leq 4 + 2/7,\end{aligned}$$

entonces, como $k \in \mathbb{Z}$,

$$k \in \{3, 4\}. \tag{18.45}$$

Por otra, de la solución general, también tenemos $y = 15 - 4k$, con $0 \leq y \leq 9$ —y es una cifra decimal—, esto es,

$$\begin{aligned} 0 \leq 15 - 4k \leq 9 &\to -15 \leq -4k \leq -15 + 9 \\ &\to 15 - 9 \leq 4k \leq 15 \\ &\to 6/4 \leq k \leq 15/4 \\ &\to 3/2 \leq k \leq 3 + 3/4 \\ &\to 1 + 1/2 \leq k \leq 3 + 3/4, \end{aligned}$$

entonces, como $k \in \mathbb{Z}$,

$$k \in \{2, 3\}. \tag{18.46}$$

De (18.45) y (18.46), $k \in \{3, 4\} \cap \{2, 3\}$, por lo que $k = 3$.

Así, $x = 30 - 7 \cdot 3 = 30 - 21 = 9$, $y = 15 - 4 \cdot 3 = 15 - 12 = 3$.

Recordemos que notamos n_2 por x y n_0 por y. Por tanto, el número $n = n_2 n_1 n_0$ es $n = 9n_1 3$; finalmente, como $n_2 + n_1 + n_0 = 20$, se tiene que $n_1 = 8$ y el número pedido es $n = 983$.

Solución.— El número pedido es 983. ■

Observación 18.15.3.— Del ejemplo anterior pudiésemos decir que, una vez descubierta la ecuación diofántica (18.42), lo hemos resuelto aplicando «teoría de ecuaciones diofánticas», lo cual supone averiguar una solución particular en función de los coeficientes de Bézout de 4 y -7 y la solución general de la ecuación diofántica; pero, una vez descubierta la ecuación diofántica, pudiésemos haber tomado otro camino, haber llegado a la solución del ejemplo aplicando «teoría de congruencias», esto es, sin calcular las soluciones particular y general anteriores.

Discusión 0.

Tenemos que

$$\begin{aligned} 4x + (-7)y = 15 &\leftrightarrow -7y = 15 - 4x \\ &\leftrightarrow 7y = 4x - 15 \\ &\leftrightarrow 7 | (4x - 15) \\ &\leftrightarrow 4x \equiv 15 \pmod{7} \\ &\leftrightarrow 4x \equiv 1 \pmod{7}, \end{aligned} \tag{18.47}$$

con $0 \leq x \leq 9$ (x es una cifra decimal).

Por el corolario 1.º del teorema de Euler-Fermat[53],

$$x \equiv 1 \cdot 4^{\varphi(7)-1} \pmod{7},$$

[53] *Vid*. teorema 18.93 (pág. 1015).

ecuación equivalente a

$$x \equiv 1 \cdot 4^{7-1-1} \pmod{7},$$

y, en definitiva, a

$$x \equiv 4^5 \pmod{7}.$$

Es conocido que $4^2 = 16 \equiv 2 \pmod{7}$, de donde, por multiplicativa con $4 \equiv 4 \pmod{7}$, tenemos $4^3 \equiv 8 \pmod{7}$ y como $8 \equiv 1 \pmod{7}$, por transitividad, $4^3 \equiv 1 \pmod{7}$ y por multiplicativa con $4^2 \equiv 2 \pmod{7}$ se sigue que $4^5 \equiv 2 \pmod{7}$; de ésta y de $x \equiv 4^5 \pmod{7}$ se sigue, por transitividad, que

$$x \equiv 2 \pmod{7},$$

y de aquí, por ser x una cifra decimal, que $x \in \{2, 9\}$.

Discusión 1.

Como alternativa a la utilización del corolario 1.º del teorema de Euler-Fermat, pudiésemos razonar de la siguiente manera.

$$\begin{aligned} 4x \equiv 1 \pmod{7} &\leftrightarrow 4x - 1 \equiv 0 \pmod{7} \\ &\leftrightarrow 7 \big| (4x - 1) \\ &\leftrightarrow 4x = \dot{7} + 1, \end{aligned}$$

con $0 \leq x \leq 9$ (x es una cifra decimal), así que los posibles valores de $4 \cdot x$ son 0, 4, 8, 16, 20, 24, 28, 32, 36; de ellos, sólo $8 = 4 \cdot 2$ y $36 = 4 \cdot 9$ son múltiplos de 7 más 1 —esto es, sólo 2 y 9 satisfacen (18.47)—.

Resolución (compleción de las discusiones).

Veamos si $x = 2$ es válido; recordemos que notamos n_2 por x, luego es la cifra de las centenas y, así, como $n_2 + n_1 + n_0 = 20$, si $n_2 = 2$, entonces $n_1 = 9$ y $n_0 = 9$ y el número sería 299, que no satisface la segunda condición, $98n_2 - 10n_1 - 199n_0 = 205$, ya que $98 \cdot 2 - 10 \cdot 9 - 199 \cdot 9 = -1685$.

También pudiésemos haber sustituido en (18.42), $4 \cdot 2 + (-7)y = 15$, de donde $y = -1$, lo cual es imposible por ser y un dígito decimal; de hecho es lo que vamos a hacer para $x = 9$; veamos que 9 es válido como valor de x utilizando (18.42): $4 \cdot 9 + (-7)y = 15$, de donde $y = 3$.

Finalmente, igual que antes, como notamos n_2 por x y n_0 por y, tenemos que el número $n = n_2n_1n_0$ es $n = 9n_13$, y como $n_2 + n_1 + n_0 = 20$, tenemos que $n_1 = 8$ y el número pedido es $n = 983$.

Observación 18.15.4.— Pudiésemos haber hecho comprobaciones con algún artefacto; por ejemplo, con Wolfram|Alpha[54]:

- con la ecuación diofántica a la que llegamos junto a las restricciones por ser cifras decimales:

```
solve 4x - 7y = 15, 0 <= x <= 9, 0 <= y <= 9 over the integers
```

- o con la formulación inicial junto a las restricciones por ser cifras decimales:

[54] *Vid.* https://www.wolframalpha.com/.

```
solve x + y + z = 20, (100x + 10y + z - 205)/2 = 100z + 10y + x, 0 <= x <= 9, 0 <= y
<= 9, 0 <= z <= 9 over the integers
```

- o sin las restricciones y quedarnos con la respuesta adecuada:

```
solve x + y + z = 20, (100x + 10y + z - 205)/2 = 100z + 10y + x over the integers
```

- o, ya en congruencias, la solución de la ecuación (esto es, dará la clase de 2 módulo 7):

```
solve 4x = 1 (mod 7)
```

que también podíamos haber solicitado el inverso de 4 módulo 7, esto es:

```
inverse of 4 mod 7
```

La equivalencia entre $4x + (-7)y = 15$ y $4x \equiv 15 \pmod{7}$ hecha en la discusión 0 de la observación 18.15.3 (pág. 1062 de esta edición) no es particular. El siguiente teorema establece la interrelación existente entre una congruencia lineal y una ecuación diofántica lineal diádica.

Teorema 18.110
$\forall a, c \in \mathbb{Z}, \forall b \in \mathbb{Z}^+$,

$$\begin{aligned} ax \equiv c \pmod{b} &\leftrightarrow b \,|\, (ax - c) \\ &\leftrightarrow (\exists y \in \mathbb{Z})(ax - c = by) \\ &\leftrightarrow (\exists y \in \mathbb{Z})(ax + (-b)y = c). \end{aligned}$$

§ 18.16 Acerca de algunas cuestiones y conjeturas famosas

Sin perjuicio de las que hayamos visto en líneas precedentes, este subcapítulo versa sobre algunas cuestiones abiertas y unas cuantas afirmaciones o negaciones aún no demostradas ni refutadas.

- **Conjetura de capicúas mediante sumas.—** Parece que data de principios del siglo XX la conjetura de que un número sumado con su reverso (el que tiene las mismas cifras en orden inverso) e iterando este proceso se llegaba a un número capicúa, por ejemplo, 39 lo consigue en dos iteraciones: $39 + 93 \mapsto 132 + 231 \mapsto 363$. A lo largo de los años se han encontrado números de los que no sabemos si originan un capicúa. El menor de ellos es 196; Wade Van Landingham los llamó *números de* Lychrel[55]: 196, 295, 394, 493, 592, 689, 691, 788, 790, 879, . . ., sucesión catalogada en la OEIS como la sucesión A023108[56]. Para saber si un número es de Lychrel, pudiésemos utilizar alguno de los verificadores en línea existentes en la RUD[57].

[55] *Vid. v. gr.* https://en.wikipedia.org/wiki/Lychrel_number.
[56] *Vid.* https://oeis.org/A023108.
[57] Por ejemplo, éste: https://www.dcode.fr/lychrel-number.

- **Número deficiente.—** Número entero positivo tal que la suma de sus partes alícuotas es menor que él, esto es, tal que

$$s(n) < n,$$

(donde $s(x)$ es la función suma alícuota —*vid. supra* definición 18.22 (pág. 987 de esta edición)—), es decir, tal que

$$\sigma(n) - n < n;$$

(donde $\sigma(x)$ es la función suma de divisores, es decir, la función divisor $\sigma_1(x)$ —*vid. supra* definición 18.21 (pág. 987 de esta edición)—); el primer número deficiente es 1. La sucesión de números deficientes, 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, . . ., está catalogada como la sucesión A005100 en la OEIS[58].

- **Número perfecto.—** Según Pitágoras (ca. 570 a. C.-ca. 490 a. C.), es un número entero positivo n que coincide con la suma de sus partes alícuotas, esto es, tal que

$$s(n) = n,$$

es decir, tal que

$$\sigma(n) - n = n;$$

el primer número perfecto es 6 ($1 + 2 + 3 = 6$), el segundo, 28 ($1 + 2 + 4 + 7 + 14 = 28$); por otra parte, Pitágoras observó que un número perfecto siempre es la suma de números enteros consecutivos, por ejemplo, el primero, 6 ($1+2+3 = 6$), el segundo, 28 ($1+2+3+4+5+6+7 = 28$), el tercero, 496 ($1 + 2 + 3 + \cdots + 30 + 31 = 496$), y que las potencias de dos son números «sólo un poco deficientes», pues la suma de los divisores de 2^n es $2^n - 1$ (por ejemplo: $1 + 2 = 2^2 - 1$, $1 + 2 + 4 = 2^3 - 1$, $1 + 2 + 4 + 8 = 2^4 - 1$); por otro lado, Euclides (ca. 325 a. C.-ca. 265 a. C.) demostró que si $2^n - 1$ es primo, entonces $2^{n-1}(2^n - 1)$ es un número par perfecto, y, por otro, Euler (1707-1783) demostró que todo número par perfecto es de la forma $2^{n-1}(2^n-1)$ con (2^n-1) primo, quedando así demostrada la equivalencia (*teorema de* Euclides-Euler[59]). La sucesión de números perfectos, 6, 28, 496, 8128, 33 550 336, 8 589 869 056, 137 438 691 328, . . ., está catalogada como la sucesión A000396 en la OEIS[60]. A fecha de hoy siguen sin respuesta varias cuestiones, entre ellas, éstas:

  ◇ ¿existen infinitos números perfectos pares?;

  ◇ ¿existe algún número perfecto impar?

[58] *Vid*. https://oeis.org/A005100.
[59] *Vid*. https://es.wikipedia.org/wiki/Teorema_de_Euclides-Euler.
[60] *Vid*. https://oeis.org/A000396.

- **Número abundante.—** Número entero positivo que es menor que la suma de sus partes alícuotas, esto es, tal que

$$n < s(n),$$

es decir, tal que

$$n < \sigma(n) - n;$$

el primer número abundante es 12 ($12 < 1 + 2 + 3 + 4 + 6 = 16$). La sucesión de números abundantes, 12, 18, 20, 24, 30, 36, 40, 42, 48, 54, 56, 60, ... (el primer número abundante impar es 945), está catalogada como la sucesión A005101 en la OEIS[61].

- **Número múltiplemente perfecto.—** Fermat notó que $\sigma(120) = 360 = 3 \cdot 120$; estos números tales que $\sigma(n) = 3n$ se llaman triplemente perfectos; en general, un número que satisface $\sigma(n) = kn$ con $k \in \mathbb{N}, k > 2$, se conoce como múltiplemente perfecto o k-perfecto (si $k = 2$, se trata de un número perfecto [observemos que $\sigma(n) = 2n \leftrightarrow \sigma(n) - n = n \leftrightarrow s(n) = n$]). A fecha de hoy sigue sin respuesta la siguiente cuestión:

  ◇ ¿existen infinitos números multiplemente perfectos?

  Observación 18.16.0.— De manera similar se define un **número múltiplemente deficiente** (o, sinónimamente, k-deficiente) como aquél que satisface $\sigma(n) < kn$ con $k \in \mathbb{N}, k > 2$, y un **número múltiplemente abundante** (o, sinónimamente, k-abundante) como aquél que satisface $kn < \sigma(n)$ con $k \in \mathbb{N}, k > 2$ (si $k = 2$, se trata de un número deficiente o abundante, respectivamente).

- **Números amigos[62].—** Decimos que m y n son números amigos (*amicable numbers*, en inglés) (o, sinónimamente, un *par amigo*) si, y sólo si,

$$s(m) = n \quad \wedge \quad s(n) = m,$$

esto es,

$$\sigma(m) - m = n \quad \wedge \quad \sigma(n) - n = m;$$

el par de números amigos más pequeños, que ya mencionó Platón, es $\langle 220, 284 \rangle$ (éstos lo son porque $D(220)\backslash\{220\} = \{1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110\}$ y $D(284)\backslash\{284\} = \{1, 2, 4, 71, 142\}$, de donde $s(220) = 284$ y $s(284) = 220$); las sucesiones más directamente relacionadas en la OEIS son la de los números amigos (A259180)[63], la de los menores de los pares de números

[61] *Vid*. https://oeis.org/A005101.
[62] No los confundamos con los *números amigables* (o, sinónimamente, *números amistosos*) (*friendly numbers*, en inglés) —*vid. v. gr.* https://en.wikipedia.org/wiki/Friendly_number—.
[63] *Vid*. https://oeis.org/A259180.

amigos (A002025)[64] y la de los mayores de los pares de números amigos (A002046)[65]. A fecha de hoy sigue sin respuesta la siguiente cuestión:

◇ ¿existen infinitos pares de números amigos?

Observación 18.16.1.— Podemos extender la condición de amistad para dos números, $s(m) = n \wedge s(n) = m$, esto es, $\sigma(m) - m = n \wedge \sigma(n) - n = m$, es decir, $\sigma(m) = \sigma(n) = m + n$ al caso de un número finito de números, $\sigma(n_0) = \sigma(n_1) = \ldots = \sigma(n_k) = n_0 + n_1 + \cdots + n_k$. De este modo, hablamos de **ternas amigas** (sucesión A125490 en la OEIS[66]) (por ejemplo, $\langle 1980, 2016, 2556 \rangle$) o de **cuaternas amigas** (sucesión A036471 en la OEIS[67]) (por ejemplo, $\langle 3270960, 3361680, 3461040, 3834000 \rangle$).

- **Números sociables.—** Decimos que $n_0, n_1, \ldots, n_{t-1}$ es una colección de números sociables de orden t (o, sinónimamente, que es una t-tupla de números sociables) si, y sólo si, constituyen un ciclo de longitud t de una sucesión alícuota[68], esto es, precisamente si existen n y k tales que

$$s^k(n) = n_0, s^{k+1}(n) = n_1, \ldots, s^{k+t-1}(n) = n_{t-1}.$$

Si la sucesión alícuota alcanza a ser constante, dicha constante es un *número perfecto* (ésta es otra forma de definir éste). Si el término inicial de dicha sucesión es un número no perfecto, se conoce como **número aspirante**. El más pequeño es 25 (su sucesión alícuota es $25, 6, 6, \ldots$). La sucesión de los números aspirantes está catalogada en la OEIS como la sucesión A063769[69]. A fecha de hoy sigue sin respuesta la siguiente cuestión:

◇ ¿es 276 un número aspirante? (En realidad, no sólo de 276 no se sabe).

La sucesión de las longitudes de las sucesiones alícuotas está catalogada en la OEIS como la sucesión A044050[70]. A fecha de hoy sigue sin respuesta la siguiente cuestión:

◇ ¿todas las sucesiones alícuotas terminan o se vuelven periódicas (se sabe que las acotadas bien terminan en 0, bien se vuelven periódicas)?[71]

Actividad 18.35

¿Existe alguna relación entre números sociables y pares amigos, ternas amigas, cuaternas amigas, etc.?

[64] *Vid.* https://oeis.org/A002025.
[65] *Vid.* https://oeis.org/A002046.
[66] *Vid.* https://oeis.org/A125490.
[67] *Vid.* https://oeis.org/A036471.
[68] *Vid. supra* definición 18.23 (pág. 987 de esta edición).
[69] *Vid.* https://oeis.org/A063769.
[70] *Vid.* https://oeis.org/A044050.
[71] *Vid. v. gr.* https://mathworld.wolfram.com/AliquotSequence.html.

- **Conjeturas de Goldbach.—** Son conocidas por este nombre un par de cuestiones que aparecieron en la correspondencia que mantuvieron Euler y Goldbach en 1742, cuyas versiones modernas son las siguientes.

  ◇ *Conjetura débil (triádica o ternaria) de* Goldbach.— Todo impar mayor que cinco es suma de tres números primos.

  Actualmente y entre muchas más cosas, con respecto a esta conjetura conocemos, por ejemplo, los siguientes teoremas.

  Teorema 18.111 (Vinográdov, 1937)
  Todo número impar suficientemente grande es suma de tres primos.

  Teorema 18.112 (Tao, 2014)
  Todo número impar puede escribirse como suma de, como mucho, cinco números primos.

  Observación 18.16.2.— ¿Ha sido ya demostrada la conjetura débil? La supuesta demostración de Helfgott (2013) de la conjetura débil aún no se ha publicado en una revista académica con revisión por pares. Por otra parte, si se aceptase esta demostración, se seguiría trivialmente la *conjetura de los primos de* Waring (que afirma que todo número impar mayor que 3 es un número primo o la suma de tres primos).

  ◇ *Conjetura (fuerte) de* Goldbach.— Todo par mayor que dos es suma de dos números primos.

  Actualmente y entre muchas más cosas, con respecto a esta conjetura conocemos, por ejemplo, los dos siguientes teoremas.

  Teorema 18.113 (Chen, 1966)
  (1966) Todo número par suficientemente grande puede escribirse como la suma de un primo y de un *casiprimo* (número que es primo o producto de dos primos).

  Teorema 18.114 (Ramaré, 1995)
  Todo número par mayor que dos puede escribirse como suma de, como mucho, seis números primos.

La conjetura (fuerte) de Goldbach implica la conjetura débil de Goldbach[72].

Observación 18.16.3.— Una novela relacionada con la conjetura fuerte de Goldbach, para pasar un buen rato (o no), es *Uncle Petros and Goldbach's Conjecture*[73] de Apostolos Doxiadis.

- **Primos gemelos.—** Par de primos que difieren sólo en dos unidades. A fecha de hoy sigue sin respuesta la siguiente cuestión:
  - ◇ ¿existen infinitos primos gemelos? (Si bien se conjetura que sí).

Observación 18.16.4.— Alphonse de Polignac[74] propone una conjetura de la cual, la conjetura de los primos gemelos es un caso particular, la ahora conocida como

- ◇ **conjetura de Polignac** (1849)[75], a saber, que para cada n entero positivo existen infinitos pares de primos consecutivos separados por $2n-1$ números compuestos,
  o de manera equivalente, que todo número par positivo es la diferencia de dos números primos consecutivos de un número infinito de maneras,
  o en otras palabras, que para todo número par positivo n, existen infinitos pares de primos consecutivos cuya diferencia es n,
  así, conjetura que existen infinitos pares de números primos separados por un número compuesto, por tres números compuestos, por cinco números compuestos, por siete números compuestos, y así sucesivamente,
  o dicho de otra forma pero equivalentemente, que existen infinitos pares de primos consecutivos cuya diferencia es dos, también infinitos cuya diferencia es cuatro, también infinitos cuya diferencia es seis, y así sucesivamente.

A modo de ejemplo:

- ◇ si $n=2$, estamos ante la *conjetura de los primos gemelos*[76]: existen infinitos pares de primos consecutivos cuya diferencia es 2: $\langle 3,5\rangle$, $\langle 5,7\rangle$, $\langle 11,13\rangle$, $\langle 17,19\rangle$, $\langle 29,31\rangle$, $\langle 41,43\rangle$, $\langle 59,61\rangle$, $\langle 71,73\rangle$, ...; las sucesiones más directamente relacionadas en la OEIS son la de los primos gemelos (A001097)[77], la de la lista de los primos gemelos (A077800)[78], la de los menores

[72] El estudio de las particiones de un número en suma de números particulares (cuadrados, cubos, primos, números triangulares, etc.) se encuadra en la conocida como *teoría aditiva de números*; en particular, es importante el estudio de la *función de partición* $p(n)$ que cuenta el número de particiones de n sin restricciones y de funciones relacionadas —por ejemplo, $p(5)=7$ ya que $5=1+1+1+1+1=1+1+1+2=1+1+3=1+2+2=1+4=2+3$—. En el capítulo de estas notas, Razonamiento combinatorio, estudiaremos el número de descomposiciones o particionamientos de un entero positivo k en n sumandos enteros no negativos, teniendo en cuenta el orden de los sumandos o no (modelización IV), resultados que podremos relacionar con el número de particiones irrestrictas $p(n)$.

[73] *Vid.* https://apostolosdoxiadis.com/book/uncle-petros-and-goldbachs-conjecture/ (en español, *vid. v. gr.* https://www.penguinlibros.com/es/literatura-contemporanea/8896-libro-el-tio-petros-y-la-conjetura-de-goldbach-9788496546561).

[74] *Vid. v. gr.* https://fr.wikipedia.org/wiki/Alphonse_de_Polignac.

[75] *Vid. v. gr.* https://fr.wikipedia.org/wiki/Conjecture_de_Polignac.

[76] *Vid. v. gr.* https://en.wikipedia.org/wiki/Twin_prime.

[77] *Vid.* https://oeis.org/A001097.

[78] *Vid.* https://oeis.org/A077800.

de los primos gemelos (A001359)[79], la de los mayores de los primos gemelos (A006512)[80] y la de la media aritmética de las parejas de primos gemelos (A014574)[81];

- si $n = 4$, se trata de la *conjetura de los primos primos*[82]: existen infinitos pares de primos consecutivos cuya diferencia es 4: $\langle 3, 7\rangle$, $\langle 7, 11\rangle$, $\langle 13, 17\rangle$, $\langle 19, 23\rangle$, ..., $\langle 739, 743\rangle$, ...; la sucesión de los miembros menores de estas parejas está catalogada como la sucesión A023200 en la OEIS[83];
- si $n = 6$, estamos ante la *conjetura de los primos sexis*[84]: existen infinitos pares de primos consecutivos cuya diferencia es 6: $\langle 5, 11\rangle$, $\langle 7, 13\rangle$, $\langle 11, 17\rangle$, $\langle 13, 19\rangle$, $\langle 17, 23\rangle$, $\langle 23, 29\rangle$, $\langle 31, 37\rangle$, $\langle 47, 53\rangle$, ..., $\langle 727, 733\rangle$, ...; la sucesión de los miembros menores de estas parejas está catalogada como la sucesión A023201 en la OEIS[85];
- si $n = 8$, se trata de la *conjetura de los primos octis*: existen infinitos pares de primos consecutivos cuya diferencia es 8: $\langle 89, 97\rangle$, $\langle 359, 367\rangle$, $\langle 389, 397\rangle$, ..., $\langle 491, 499\rangle$, ...; la sucesión de los miembros menores de estas parejas está catalogada como la sucesión A023202 en la OEIS[86].

En definitiva, recordemos la conjetura de POLIGNAC (1849): para todo número par positivo n existen infinitos pares de números primos consecutivos cuya diferencia es n.

A día de hoy sigue sin haber sido ni refutada ni demostrada (de haber sido demostrada, sería un teorema y no una conjetura).

Sin embargo: Yitang ZHANG demostró en abril de 2013 que existen infinitas parejas de números primos cuya separación no es mayor que 70 000 000; en mayo, esta cota ya se había rebajado a 59 470 640; a finales de julio, un proyecto Polymath con Terence TAO la rebajó a 4680; en noviembre, James MAYNARD consiguió rebajarla a 600; en abril de 2014, el proyecto Polymath consiguió rebajarla a 246, y sin hacer intervenir a ninguna conjetura aquí es donde estamos a fecha de hoy, en el siguiente teorema.

Teorema 18.115

Existen infinitas parejas de primos consecutivos cuya diferencia es como mucho 246.[87]

- **Primalidad de $2^p - 1$.—** Si $2^p - 1$ es primo, p es primo; $p = 11$ es el primer primo para el que no es cierta la inversa: $2^{11} - 1 = 2047 = 23 \cdot 89$.

[79] *Vid.* https://oeis.org/A001359.
[80] *Vid.* https://oeis.org/A006512.
[81] *Vid.* https://oeis.org/A014574.
[82] *Vid. v. gr.* https://en.wikipedia.org/wiki/Cousin_prime.
[83] *Vid.* https://oeis.org/A023200.
[84] *Vid. v. gr.* https://en.wikipedia.org/wiki/Sexy_prime.
[85] *Vid.* https://oeis.org/A023201.
[86] *Vid.* https://oeis.org/A023202.
[87] Admitiendo la *conjetura de* ELLIOTT-HALBERSTAM (más allá de los márgenes de estas notas), James MAYNARD, en noviembre de 2013, redujo la cota a 12; admitiendo la *conjetura de* ELLIOTT-HALBERSTAM *generalizada*, el proyecto Polymath, en agosto de 2014, rebajó dicha cota a 6.

- **Número primo de Mersenne.—** Número primo de la forma $2^p - 1$ con p primo; los mayores primos conocidos en la actualidad son primos de Mersenne (1588-1648). A fecha de hoy sigue sin respuesta la siguiente cuestión:
  - ¿existen infinitos primos de Mersenne? (observemos que esto equivale a preguntarnos por la existencia de infinitos números perfectos pares).
- **Prueba de primalidad de Lucas.—** $2^p - 1$ es primo si, y sólo si, $2^p - 1$ divide al término s_{p-1} de la sucesión $s_0 = 4$, $s_n = s_{n-1}^2 - 1$; Lucas demostró con él, en 1876, que $2^{127} - 1$ es primo (hasta esa fecha, el mayor primo de Mersenne conocido era $2^{31} - 1$ —hecho que demostró Euler—).
- **Número de Fermat.—** Número entero positivo de la sucesión $F_n = 2^{2^n} + 1$; $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$ —estos cinco primeros son primos y Fermat (1601-1665) conjetura que lo son todos—, $F_5 = 4\,294\,967\,297$ (Euler, en 1732, demuestra que éste es divisible por 641 y por tanto, compuesto, refutando así la conjetura de Fermat); satisfacen la recurrencia $F_{n+1} = F_0 \cdot F_1 \cdot \ldots \cdot F_n + 2$; Gauss demostró que estos primos determinan los polígonos regulares que son construibles con regla y compás, concretamente: un polígono regular es construible con regla y compás si, y sólo si, su número de lados es igual al producto de una potencia de dos por un producto de números de Fermat primos diferentes. A fecha de hoy sigue sin respuesta la siguiente cuestión:
  - ¿existen infinitos números de Fermat primos? (Se conjetura que no, que los únicos son F_0, F_1, F_2, F_3 y F_4 —sin embargo, a fecha de hoy, tampoco se sabe si existen infinitos números de Fermat compuestos—).
- **Una más.—** ◇ ¿Existen infinitos primos de la forma $n^2 + 1$?
- **Otra más.—** ◇ Entre dos cuadrados, ¿existe siempre un primo?
- **Número primo de Sophie Germain.—** Número primo p tal que $2p + 1$ también es primo;
  - se conjetura que existen infinitos primos de Germain (1776–1831).
- **Conjetura de Singmaster.—.—** ¿Existe algún número natural mayor que 1 que aparezca más de 8 veces en el triángulo de Pascal-Tartaglia [88]?
  - Singmaster conjetura que existe una cota superior global N al número de apariciones (esto es, que todos los números aparecen menos de N veces) y que N es 10 o como mucho 12.
- **Conjetura de Erdős-Straus.—.—** Si $n \in \mathbb{Z}$, $n \geq 2$, entonces existen enteros positivos x, y, z tales que $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$.

[88] *Vid. infra* pág. 1130 de esta edición.

§ 18.17 Tres ejemplos de conjeturas que dejaron de serlo

Dos porque se han convertido en teoremas:

Teorema 18.116 (Último teorema de FERMAT)
(Conjeturado por FERMAT en 1637 y demostrado por WILES en 1995).
Si n es un número entero mayor que dos, entonces no existen números enteros positivos x, y, z tales que $x^n + y^n = z^n$.

Teorema 18.117 (Teorema de MIHĂILESCU)
(Anteriormente, *conjetura de* CATALAN, ya que fue conjeturado por éste en 1884), (demostrado por MIHĂILESCU en 2002).
Las únicas potencias de enteros positivos cuya diferencia es una unidad son 8 y 9 (2^3 y 3^2), esto es, la única solución de la ecuación diofántica $x^m - y^n = 1$, con $x, y > 0$, $m, n > 1$ es $m = 2$, $n = 3$, $x = 3$, $y = 2$ ($3^2 - 2^3 = 1$).

Una porque se ha demostrado su falsedad[89]:

Teorema 18.118 (Refutación de la conjetura de EULER sobre la suma de potencias)
(Conjeturada por EULER en 1769 y refutada por LANDER y PARKIN en 1966)[a].
No es cierta la conjetura de EULER sobre la suma de potencias, a saber, no es cierto que para todo entero $n \geq 2$ sean necesarias al menos n potencias enésimas para que su suma sea también una potencia enésima.

[a] *Vid. v. gr.* https://es.wikipedia.org/wiki/Conjetura_de_Euler.

Demostración.— La refutación de LANDER y PARKIN[90]: $27^5 + 84^5 + 110^5 + 133^5 = 144^5$. ■

Observación 18.17.0.— A propósito de este último, en 1967, LANDER, PARKIN y SELFRIDGE, propusieron una conjetura relacionada de la que aún no sabemos de su certeza (*vid. v. gr.* https://fr.wikipedia.org/wiki/Conjecture_de_Lander-Parkin-Selfridge).

[89] Un artículo muy sugerente relacionado con algunas conjeturas refutadas es *Un millón de casos no bastan: hace falta una demostración* de Juan Luis VARONA, https://www.unirioja.es/cu/jvarona/downloads/Un-millon-de-casos-no-bastan-MatMat.pdf.

[90] *Vid. v. gr.* https://www.openculture.com/2015/04/shortest-known-paper-in-a-serious-math-journal.html.

§ 18.18 Números y lingüística natural humana

Definición 18.36.— Llamamos *número normal* a todo número real en el que toda secuencia finita de números naturales figura en su desarrollo decimal.

Ejemplo 586

Demostremos que todo número normal contiene toda la producción lingüística natural humana habida y por haber.

Resolución.— Si suponemos que toda lengua natural humana se basa en un alfabeto finito, entonces como toda secuencia finita de palabras de una lengua natural humana puede codificarse por una secuencia finita de números naturales, todo número normal contiene toda la producción lingüística natural humana habida y por haber. ■

Definición 18.37.— Llamamos *número nombrable* a todo número real describible por una secuencia finita de palabras de una lengua natural humana.

Ejemplo 587

Demostremos que existe un número infinito no numerable de números reales no describibles por secuencias finitas de palabras.

Resolución.— En efecto, como el número de secuencias finitas es infinito numerable, existe un número infinito no numerable de números reales no describibles por secuencias finitas de palabras. ■

Ejemplo 588

Demostremos que todos los números reales son describibles por subconjuntos de secuencias finitas de palabras.

Resolución.— En efecto, como el número de subconjuntos de secuencias finitas de palabras es infinito no numerable —por el teorema de CANTOR—, entonces, sí que todos los números reales son describibles por subconjuntos de secuencias finitas de palabras. ■

§ 18.19 Fundamentos lógicos y numéricos de la programación de computadores

La *lógica de juntores* tiene sus correspondientes en el álgebra de BOOLE, una *lógica algebraica* y en la *lógica combinacional*, en electrónica digital, que implementa mediante circuitos eletrónicos operaciones booleanas. Estas lógicas carecen de memoria, son independientes del tiempo en el sentido de que el resultado de una función lógica depende únicamente de sus argumentos —no ocurre esto con la *lógica secuencial*, dependiente del tiempo, con memoria, lógica que se usa por ejemplo, para la construcción de *máquinas de estado finito*, en la que el resultado de una función lógica depende de sus argumentos y de llamadas a la misma función (y quizás a otras) con argumentos anteriores en la ordenación (posiblemente en sentido temporal), esto es, el resultado depende tanto del estado actual de la máquina como de los anteriores, ya que aquél está determinado por éstos.

§ 18.20 Muestra de más ejemplos

Ejemplo 589

Demostremos que $16! + 23^{16}$ es divisible por 17.

[EFO 17.1.2022:5a], [PEP 5.4.2022:5a]. *Cfr.* GARCÍA, HERNÁNDEZ y NEVOT [150]: problema resuelto 1.59 (págs. 38–39).

Resolución.— Demostremos que $16! + 23^{16} \equiv 0 \pmod{17}$. Por una parte, como 17 es primo, entonces, por el teorema de WILSON (*vid. supra* teorema 18.97 [pág. 1025 de esta edición]),

$$(17-1)! \equiv -1 \pmod{17},$$

esto es,

$$16! \equiv -1 \pmod{17}. \tag{18.48}$$

Por otra, como 17 y 23 son primos entre sí, entonces, por el corolario 2.º del teorema de EULER-FERMAT (*vid. supra* teorema 18.91 [pág. 1013 de esta edición]),

$$23^{17-1} \equiv 1 \pmod{17},$$

es decir,

$$23^{16} \equiv 1 \pmod{17}. \tag{18.49}$$

Finalmente, de (18.48) y (18.49), por la propiedad aditiva (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) de las congruencias, sumándolas miembro a miembro, obtenemos

$$16! + 23^{16} \equiv 0 \pmod{17},$$

en otras palabras, que $16! + 23^{16}$ es divisible por 17. ■

Ejemplo 590

Calculemos el resto de dividir $3^{2n+2} + 2^{6n+1} - 7$ por 11, para cualquier $n \in \mathbb{N}$.

[PEP 10.4.2019:4b].

Resolución.— Veamos.

$$\begin{aligned} 3^{2n+2} + 2^{6n+1} &\equiv 3^2 \cdot 3^{2n} + 2 \cdot 2^{6n} && \pmod{11} \\ &\equiv 3^2 \cdot (3^2)^n + 2 \cdot (2^6)^n \\ &= 9 \cdot 9^n + 2 \cdot 64^n && \pmod{11} \\ &\equiv 9 \cdot 9^n + 2 \cdot 9^n && \pmod{11} \\ &= (9+2) \cdot 9^n \\ &= 11 \cdot 9^n \\ &\equiv 0 && \pmod{11}. \end{aligned}$$

En definitiva,

$$3^{2n+2} + 2^{6n+1} \equiv 0 \pmod{11}. \tag{18.50}$$

Como $-7 \in [4]_{\text{mód } 11}$, la clase de equivalencia de 4 módulo 11 (si contásemos hacia atrás 7 desde 11 llegaríamos a 4),

$$-7 \equiv 4 \pmod{11}. \tag{18.51}$$

Finalmente, de (18.50) y (18.51), por la propiedad aditiva (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) de las congruencias, sumándolas miembro a miembro, obtenemos

$$3^{2n+2} + 2^{6n+1} - 7 \equiv 4 \pmod{11}.$$

Solución.— Para cualquier $n \in \mathbb{N}$, el resto de dividir $3^{2n+2} + 2^{6n+1} - 7$ por 11 es 4. ■

Ejemplo 591

¿Cuáles son los $n \in \mathbb{Z}$, múltiplos de 5 cuyo resto al dividirlos por 7 es 1? Expresemos la respuesta en función de un parámetro, $n = f(t)$, $\forall t \in \mathbb{Z}$ (así, por ejemplo, ..., $f(-1) = -20$, $f(0) = 15$, $f(1) = 50$, ...).

[EFO 17.1.2022:5b], [PEP 5.4.2022:5b]. *Cfr.* García, Hernández y Nevot [150]: problema resuelto 1.48 (pág. 33).

Resolución.— Por un lado, los enteros múltiplos de 5 son de la forma $n = 5k$, con $k \in \mathbb{Z}$. Por el otro, $n \equiv 1 \pmod 7$. De ambos, tenemos que $\exists k \in \mathbb{Z}$ tal que

$$5k \equiv 1 \pmod 7,$$

de donde, por la propiedad de las congruencias, producto por un escalar entero (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) (en este caso, $3 \in \mathbb{Z}$),

$$3 \cdot 5 \cdot k \equiv 3 \cdot 1 \pmod 7. \tag{18.52}$$

Por otra parte, como en $\mathbb{Z}_7$, 3 y 5 son simétricos multiplicativos, esto es, en particular,

$$3 \cdot 5 \equiv 1 \pmod 7,$$

entonces, de nuevo, por la propiedad producto por un escalar entero ($k \in \mathbb{Z}$),

$$3 \cdot 5 \cdot k \equiv 1 \cdot k \pmod 7,$$

que por la simetría de la relación $\equiv \pmod 7$, equivale a

$$1 \cdot k \equiv 3 \cdot 5 \cdot k \pmod 7. \tag{18.53}$$

De (18.53) y (18.52), por la transitividad de la relación $\equiv \pmod 7$,

$$k \equiv 3 \pmod 7,$$

en otras palabras,

$$\begin{aligned} k \in [3]_{(7)} &= \{\dots, -25, -18, -11, -4, 3, 10, 17, 24, \dots\} \\ &= \{3 + 7t : t \in \mathbb{Z}\}, \end{aligned}$$

por lo que

$$\begin{aligned} n &= 5k \\ &= 5 \cdot (3 + 7t) \end{aligned}$$

$$= 15 + 35t, \text{ con } t \in \mathbb{Z}.$$

Solución.— Los $n \in \mathbb{Z}$, múltiplos de 5 cuyo resto al dividirlos por 7 es 1 son precisamente los del conjunto $\{n = 15 + 35t : t \in \mathbb{Z}\}$, esto es, $\{\ldots, 15 + 35 \cdot (-1), 15 + 35 \cdot 0, 15 + 35 \cdot 1, \ldots\}$, es decir, $\{\ldots, -20, 15, 50, \ldots\}$. ■

Ejemplo 592

Demostremos que el número 8 divide al producto de cualesquiera dos naturales pares consecutivos.

Resolución.— Demostrémoslo por dos vías.

Vía 0.

Veamos que 4 divide necesariamente a uno de dichos pares. Demostrémoslo por inducción débil.

En efecto, un número natural m producto de dos pares consecutivos es de la forma $m = 2k(2k+2)$ para algún $k \in \mathbb{N}$. Sea $P(k) \leftrightharpoons 4|2k$ o $4|(2k+2)$. Apliquemos inducción débil (*cfr. supra* teorema 16.0 —pág. 805—):

Caso base (ID_0).— $P(0)$ se satisface, ya que $4|0$.

Paso inductivo (ID_1).— Supongamos $P(k)$, esto es, $4|2k$ o $4|(2k+2)$, y preguntémonos $P(k+1)$, es decir, $4|(2k+2)$ o $4|(2(k+1)+2)$; pues bien, si $4|2k$, entonces $4|(2(k+1)+2)$ ya que este último es precisamente $2k+4$; por otra parte, si $4|(2k+2)$, entonces $4|(2k+2)$; en definitiva, de $P(k)$ se sigue $P(k+1)$.

Conclusión ($ID_0 \wedge ID_1$).— Como se satisfacen el caso base y el paso inductivo, entonces, por el teorema 16.0 (pág. 805 de esta edición), de inducción débil, se tiene lo buscado, a saber, que $\forall k \in \mathbb{N}$, $4|2k$ o $4|(2k+2)$. □

Vía 1.

Sean $2n$ y $(2n+2)$ dos naturales pares consecutivos arbitrarios. El producto es divisible por 8 porque $\forall n \in \mathbb{Z}, 2n \cdot (2n+2) = 4n(n+1)$ y como el producto de dos números consecutivos $n \cdot (n+1)$ es múltiplo de 2 (pues dividir por 2 solo genera un resto no nulo, en otras palabras, o bien n es par o bien $n+1$ es par), se tiene que $n(n+1)$ es de la forma $2k$ con k entero y por tanto, $2n \cdot (2n+2) = 4n(n+1) = 4 \cdot 2k = 8 \cdot k$, esto es, múltiplo de 8. ■

Ejemplo 593

Demostremos que el número 3 divide al producto de tres números naturales consecutivos cualesquiera.

Resolución.— De hecho, esto se deduce de que la división euclidea por 3 sólo tiene dos restos distintos de cero. En efecto, sea $m \cdot (m+1) \cdot (m+2)$; si $3 \nmid m$, entonces $m = 3k+1$ o $m = 3k+2$, pero, si $m = 3k+1$, $3 \mid (m+2)$ ya que $m+2 = 3k+3$, y si $m = 3k+2$, $3 \mid (m+1)$ ya que $m+1 = 3k+3$. ■

Ejemplo 594

Demostremos que para todo número natural impar n se satisface que el número $n^3 - n$ es divisible por 24.

ⓘ Recordemos que es buena costumbre demostrar las afirmaciones intermedias que hagamos, por muy evidentes que nos parezcan; no las dejemos en meras conjeturas.

[EFE 28.6.2023:5], [SEL 6:7]. *Cfr.* Anzola y Caruncho [197]: problema 7.19 (pág. 146).

Resolución.— Resulta que $n^3 - n$ es producto de tres números naturales consecutivos. En efecto,

$$\begin{aligned} n^3 - n &= n(n^2 - 1) \\ &= (n-1)n(n+1). \end{aligned} \tag{18.54}$$

Además, observemos que como n es impar, $n-1$ y $n+1$ son pares.

Debemos demostrar que $24 \mid (n^3 - n)$. Como $24 = 8 \cdot 3$, que 24 divida a $(n^3 - n)$ equivale a que lo dividan 8 y 3. En definitiva, nuestro objetivo es demostrar que $8 \mid (n^3 - n)$ y que $3 \mid (n^3 - n)$.

Por una parte, la factorización (18.54) incluye el producto de los naturales pares consecutivos $n-1$ y $n+1$. El ejemplo 592 (pág. 1077 de esta edición) nos asegura que 8 divide a tal producto, esto es, que $8 \mid (n-1)(n+1)$. Como $(n-1)(n+1) \mid (n^3 - n)$, entonces, de la transitividad de $\mid$, se sigue que $8 \mid (n^3 - n)$.

Por otra, la factorización (18.54) incluye el producto de los tres números naturales consecutivos $n-1$, n y $n+1$. El ejemplo 593 (pág. 1078 de esta edición) nos asegura que 3 divide a tal producto, esto es, que $3 \mid (n^3 - n)$.

Por lo tanto, $24 \mid (n^3 - n)$. ■

Ejemplo 595

Demostremos que si n es un número natural par, entonces 48 divide a $n(n^2+20)$.

[EFO 4.6.2021:5b]. *Cfr.* Anzola y Caruncho [197]: problema 7.81 (pág. 172).

Resolución.— En efecto,

$$\begin{aligned} n(n^2+20) &= n(n^2-4+24) \\ &= n(n^2-4)+24n \\ &= n(n-2)(n+2)+24n. \end{aligned} \tag{18.55}$$

- *Análisis del primer sumando,* $n(n-2)(n+2)$.

  Como n es par, $n-2$ y $n+2$ también lo son, por lo que el primer sumando de (18.55), $(n-2)n(n+2)$, es el producto de tres pares consecutivos.

  Demostremos que sucede que el producto de tres números naturales pares consecutivos es múltiplo de 48 (por lo que este primer sumando es múltiplo de 48). Lo hacemos por tres vías.

  Vía 0.

  Por el ejemplo 592 (pág. 1077 de esta edición), 8 divide al producto de tres números naturales pares consecutivos, pues divide al de dos; pero fijémonos, 8 divide al producto de los dos primeros y como el tercero es par, 2 divide a éste, por lo que $8\cdot 2$, esto es, 16, divide al producto de los tres. Por otro lado, el ejemplo 593 (pág. 1078 de esta edición), 3 divide al producto de tres números naturales pares consecutivos, pues divide al de cualesquiera tres naturales consecutivos. En consecuencia, $16\cdot 3$, esto es, 48, divide al producto de los tres. □

  Vía 1.

  El producto $0\cdot 2\cdot 4$ es múltiplo de 48 por serlo 0. Sea n un natural positivo y sean $2n$, $2n+2$ y $2n+4$ los tres pares consecutivos (el primer producto es $2\cdot 4\cdot 6$). Su producto, $2n(2n+2)(2n+4)$ es múltiplo de 16 porque necesariamente[91] uno de los pares es múltiplo de 4; por otra parte, uno de ellos necesariamente[92] es múltiplo de 3 y, por tanto, el producto de los tres es múltiplo de 48 ($=16\cdot 3$). □

[91] Dados n o más números consecutivos, alguno de ellos es múltiplo de n, ya que por el algoritmo de la división al dividir entre n hay n restos posibles, del resto 0 al resto $n-1$ y es precisamente el resto 0 el que corresponde a los múltiplos de n. En el caso que nos ocupa, tres números pares consecutivos corresponden a cinco números naturales consecutivos, por lo que hay, en particular, 4 números naturales consecutivos, de donde alguno de los cuales es múltiplo de 4, y como para ser múltiplo de 4 debe ser par, pues alguno de los susodichos pares es múltiplo de 4.

[92] Sea $2n=3k+r$ y, por tanto, $2n+2=3k+r+2$ y $2n+4=3k+r+4$; por el algoritmo de la división, r es 0, 1 o 2; si $r=0$, entonces $3\mid 2n$; si $r=1$, entonces $3\mid(2n+2)$; si $r=2$, entonces $3\mid(2n+4)$.

Vía 2.

El producto de k números naturales consecutivos es múltiplo de $k!$, pues $(n+1)\cdot(n+2)\cdot \ldots \cdot (n+k) = \binom{n+k}{n} \cdot k!$ (el producto $0 \cdot 2 \cdot 4$ también es múltiplo de $k!$ por serlo 0). Si escribimos el producto de los tres naturales pares como $(2n+2)(2n+4)(2n+6)$, éste es igual a $8(n+1)(n+2)(n+3)$, que es múltiplo de $8 \cdot 3! = 48$. □

- *Análisis del segundo sumando,* $24n$.

  Por ser n par, esto es, $n = 2k$ con k natural, entonces el segundo sumando de (18.55), $24n = 24 \cdot 2 \cdot k = 48 \cdot k$, es decir, es múltiplo de 48.

Por lo tanto, como ambos sumandos de (18.55), $n(n-2)(n+2)$ y $24n$, son múltiplos de 48, se tiene que $n(n^2+20)$ es múltiplo de 48. ■

Ejemplo 596

Demostremos que el cuadrado de un número impar es impar.

Resolución.— Observemos que $\forall n \in \mathbb{Z}$, $(2n+1)^2 = 4n^2+4n+1 = 2(2n^2+2n)+1$, es decir, es de la forma $2k+1$ con k entero. ■

Ejemplo 597

Demostremos que $\forall n \in \mathbb{N}$ se satisface que si n es impar, entonces $16 \,|\, (n^4-1)$.

[PEP 10.4.2019:4a].

Resolución.— Ante todo, $n^4-1 = (n^2+1)(n^2-1) = (n^2+1)(n+1)(n-1)$; entonces:

- por una parte, como n es impar y $n-1$ y $n+1$ son dos pares consecutivos, su producto es múltiplo de 8 (*vid. supra* ejemplo 592 [pág. 1077 de esta edición]), por lo que n^4-1 también lo es;
- por otra, como n es impar, su cuadrado es impar (*vid. supra* ejemplo 596 [pág. 1080 de esta edición]), de donde n^2+1 es par, esto es, múltiplo de 2.

La conjunción de ambos resultados demuestra que n^4-1 es múltiplo de $8 \cdot 2 = 16$. ■

Ejemplo 598

¿Qué resto se obtiene al dividir 2963^{1103} por 9?

[Cubit 133].

Resolución.— No nos dicen nada del sistema de numeración, pero según las cifras que vemos lo más simple es suponer que los números están en base 10.

Pudiésemos pensar en hallar un criterio de divisibilidad por 9 en base 10; y pudiésemos emplear el criterio general de divisibilidad; así:

$$10^0 \equiv 1 \pmod 9, \text{ por lo que } r_0 = 1;$$
$$10^1 \equiv 1 \pmod 9, \text{ por lo que } r_1 = 1,$$

y los restos se repiten de forma periódica, por tanto, la sucesión de restos potenciales sucesivos de 10 módulo 9, $r_0, r_1, r_2, \ldots$, es $1, 1, 1, \ldots$ (no hay residuos en la parte no periódica porque 10 y 9 son primos entre sí).

Aplicando el criterio general de divisibilidad en base 10, a saber,

$n = n_k \ldots n_2 n_1 n_0$ es divisible por 9 si, y sólo si, $n_0 r_0 + n_1 r_1 + n_2 r_2 + \cdots + n_k r_k$ es divisible por 9,

esto es, si, y sólo si,

$n_0 + n_1 + n_2 + n_3 + \cdots$ es divisible por 9,

en palabras: en base 10, un número es divisible por 9 si, y sólo si, la suma de sus cifras es divisible por 9.

Bueno, y todo esto, ¿para qué? Hemos explorado, ¿y …?

A ver, intentemos otro camino.

Hallemos los restos potenciales sucesivos de 2963 respecto al módulo 9, es decir,

$$2963^0 \equiv 1 \pmod 9, \text{ por lo que } r_0 = 1,$$
$$2963^1 \equiv 2 \pmod 9, \text{ por lo que } r_1 = 2,$$
$$2963^2 = 2963^1 \cdot 2963^1 \equiv 2 \cdot 2 = 4 \pmod 9, \text{ por lo que } r_2 = 4,$$
$$2963^3 = 2963^1 \cdot 2963^2 \equiv 2 \cdot 4 = 8 \pmod 9, \text{ por lo que } r_3 = 8,$$
$$2963^4 = 2963^1 \cdot 2963^3 \equiv 2 \cdot 8 = 16 \equiv 7 \pmod 9, \text{ por lo que } r_4 = 7,$$
$$2963^5 = 2963^1 \cdot 2963^4 \equiv 2 \cdot 7 = 14 \equiv 5 \pmod 9, \text{ por lo que } r_5 = 5,$$
$$2963^6 = 2963^1 \cdot 2963^5 \equiv 2 \cdot 5 = 10 \equiv 1 \pmod 9, \text{ por lo que } r_6 = 1 = r_0,$$

y los restos potenciales sucesivos comienzan a repetirse de forma periódica.

Por otro lado,

$$\begin{aligned} 2963^{1103} &= 2963^{6\cdot183+5} \\ &= 2963^{6\cdot183} \cdot 2963^5 \end{aligned}$$

$$= (2963^6)^{183} \cdot 2963^5.$$

Así, como $2963^6 \equiv 1 \pmod 9$, entonces, por la propiedad de potencia (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) de las congruencias, $(2963^6)^{183} \equiv 1^{183} \pmod 9$, esto es,

$$(2963^6)^{183} \equiv 1 \pmod 9,$$

de donde, por la propiedad multiplicativa (*vid. supra* teorema 18.68 [pág. 992 de esta edición]) de las congruencias, $(2963^6)^{183} \cdot 2963^5 \equiv 1 \cdot 2963^5 \pmod 9$, esto es,

$$(2963^6)^{183} \cdot 2963^5 \equiv 2963^5 \pmod 9, \tag{18.56}$$

y como

$$2963^5 \equiv 5 \pmod 9, \tag{18.57}$$

entonces, por la propiedad transitiva de la relación de equivalencia $\equiv \pmod 9$ aplicada a (18.56) y (18.57),

$$(2963^6)^{183} \cdot 2963^5 \equiv 5 \pmod 9.$$

Solución.— El resto que se obtiene al dividir 2963^{1103} por 9 es 5. ■

Ejemplo 599

¿Cuál es el menor número entero positivo cuyo producto por 33 da un número con todas sus cifras iguales a 7?

[Cubit 123].

Resolución.— Al no decir nada, suponemos que se trata del sistema de numeración decimal (base 10).

Sea n un entero positivo tal que $33n = 77\ldots7$, de donde $33n = 7 \cdot 11\ldots1$, por lo que 33 es un divisor de $7 \cdot 11\ldots1$ y de aquí, al ser 33 y 7 coprimos, deducimos que 33 es un divisor de $11\ldots1$.

Busquemos ahora el menor múltiplo de 33 de la forma $11\ldots1$. Por ser múltiplo de 33 , debe serlo de 3 y de 11. Entonces:

- por un lado, por el criterio de divisibilidad por 3, para ser múltiplo de 3, la suma de sus cifras debe ser múltiplo de 3, lo que para un número de la forma $11\ldots1$ significa que su número de cifras debe ser múltiplo de 3;
- por otro, el criterio de divisibilidad por 11 aplicado a un número de la forma $11\ldots1$ implica que este número debe tener un número par de cifras, ya que la suma alternada $(1-1)+(1-1)+\cdots+(1-1)$ debe ser múltiplo de 11.

Así, de tener que ser el número de cifras, múltiplo de 3, el menor posible y par, deducimos que el número de cifras es 6, el número es 111 111 y por tanto, $n = 777\,777/33 = 23\,569$.

Solución.— El menor número entero positivo cuyo producto por 33 da un número con todas sus cifras iguales a 7 es 23 569. ■

Ejemplo 600

Un robot se mueve hacia adelante dando saltos de exactamente 2 m (salto corto) o 3 m (salto largo), perfectamente alineados en horizontal. Si tiene que recorrer 23 m en línea recta, calculemos cuántos saltos cortos y cuántos saltos largos debe dar, siendo el número total de saltos (cortos + largos) el menor posible.

[EFO 3.6.2019:3]. *Cfr.* ANZOLA y CARUNCHO [197]: problema 8.5 (pág. 183).

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Si x e y representan el número de saltos de 2 m y el de 3 m, respectivamente, entonces, se tiene que la siguiente ecuación representa lo expuesto en el enunciado salvo la condición de minimización:

$$2x + 3y = 23.$$

Esta ecuación es irreducible en los enteros —2, 3 y 23 son números primos y, por tanto, (mutuamente) coprimos—. Como se buscan soluciones enteras, se tiene así una ecuación diofántica, con dos variables.

II. *Demostración de que tiene al menos una solución.*

¿Tiene solución entera? Sí, por el teorema 18.107 (pág. 1047 de esta edición), pues $\mathrm{mcd}(2,3) = 1 \mid 23$.

III. *Cálculo de una solución particular.*

Coeficientes de BÉZOUT: por simple inspección, $s = -1$ y $t = 1$ (pudiésemos hallarlos también con el algoritmo de EUCLIDES hacia atrás o con el algoritmo de EUCLIDES extendido).

Una solución particular es

$$x_0 = \frac{23 \cdot (-1)}{1} = -23,$$
$$y_0 = \frac{23 \cdot 1}{1} = 23.$$

Comprobación.— En efecto, $2 \cdot (-23) + 3 \cdot 23 = 23$.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general es

$$\begin{aligned} x &= -23 + \frac{k}{1} \cdot 3 \\ &= -23 + 3k, \\ y &= 23 + \frac{k}{1} \cdot (-2) \\ &= 23 - 2k, \end{aligned}$$

para $k \in \mathbb{Z}$.

Comprobación.— En efecto, $2 \cdot (-23 + 3k) + 3 \cdot (23 - 2k) = 2 \cdot (-23) + 6k + 3 \cdot 23 - 6k = 23$.

V. *Cálculo de la solución de la cuestión en estudio.*

Encontremos finalmente la solución concreta de la cuestión en estudio. Para ello, intentemos acotar k. Como 23 no es divisible ni por 2 ni por 3 (23 es un número primo), es seguro que en recorrer los 23 m van a intervenir saltos de 2 m y de 3 m, esto es: $x > 0$ e $y > 0$ y así:

$$\begin{aligned} 0 < x &\to 0 < -23 + 3k \\ &\to 23 < 3k, \\ &\to \frac{23}{3} < k, \\ 0 < y &\to 0 < 23 - 2k \\ &\to -23 < -2k \\ &\to k < \frac{23}{2} \\ &\to k \in \{8, 9, 10, 11\}, \end{aligned}$$

Se tienen entonces los siguientes valores para x e y según los valores de k:

$k =$	8	9	10	11
$x = -23 + 3k =$	1	4	7	10
$y = 23 - 2k =$	7	5	3	1
N.º total de saltos =	8	9	10	11

Solución.— Para recorrer 23 m con el menor número total de saltos posible, el robot debe hacer un salto de 2 m y siete saltos de 3 m en cualquier orden. ■

Observación 18.20.0.— Si estuviésemos interesados en saber el número de formas en que puede recorrer los 23 m en estas condiciones, la solución sería el número de tuplas de la forma $\langle 2, 3\rangle_{1,7}$[93],

[93] Empleamos una notación similar a la que mencionamos en la observación 12.7.0 (pág. 705 de esta edición) para multiconjuntos; tuplas de la forma $\langle 2, 3\rangle_{1,7}$ son, por ejemplo, $\langle 2, 3, 3, 3, 3, 3, 3, 3\rangle$, $\langle 3, 3, 3, 2, 3, 3, 3, 3\rangle$ y $\langle 3, 3, 3, 3, 3, 3, 2, 3\rangle$.

esto es, el número total de permutaciones con repetición[94],

$$\mathrm{PR}_{1,7} = \frac{(1+7)!}{1! \cdot 7!} = 8,$$

correspondientes a las diferentes posiciones del salto de 2 m, delante (una), entre (seis) y después (una) de los 7 saltos de 3 m.

Ejemplo 601

Supongamos que una persona debe gastar exactamente 1234 euros en comprar objetos de dos tipos. Los objetos de tipo A cuestan 12 euros y los de tipo B, 34 euros, cada uno. Si dicha persona debe comprar al menos un objeto de cada tipo, entonces, usando la teoría de ecuaciones diofánticas, averigüemos cuántos objetos de tipo A y B puede comprar. Proporcionemos todas las soluciones existentes.

[EFE 7.7.2017:4], [SEL 7:3]. *Cfr.* González [153]: ejemplo 12.8 (pág. 353).

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Sean x el número de objetos de tipo A e y el número de objetos de tipo B; entonces lo expuesto en el enunciado se formaliza como

$$12x + 34y = 1234, \tag{18.58}$$

sujeto a las restricciones de que $x > 0$ e $y > 0$.

II. *Demostración de que tiene al menos una solución.*

Por el algoritmo de Euclides, el $\operatorname{mcd}(12, 34)$,

$$34 = 2 \cdot 12 + 10, \tag{18.59}$$

$$12 = 1 \cdot 10 + 2, \tag{18.60}$$

$$10 = 5 \cdot 2 + 0,$$

donde comprobamos que el resto anterior al nulo vale 2.

Por lo establecido en el teorema 18.107 (pág. 1047 de esta edición), esta ecuación diofántica tiene solución entera, ya que $\operatorname{mcd}(12, 34) = 2$ divide a 1234.

III. *Cálculo de una solución particular.*

[94] *Vid.* § 19.2.4 (pág. 1163 de esta edición).

De (18.60),

$$\begin{aligned} 2 &= 12 - 10 \cdot 1 \\ &= 12 - (34 - 12 \cdot 2) \cdot 1 \\ &= 12 \cdot 3 + 34 \cdot (-1), \end{aligned}$$

por lo que los coeficientes de Bézout s y t son 3 y -1, respectivamente, esto es, una solución —particular— de $12x + 34y = 2$ es $\langle x, y \rangle = \langle 3, -1 \rangle$.

Una solución —particular— de (18.58) es

$$\begin{aligned} x_0 &= \frac{3 \cdot 1234}{2} = 1851, \\ y_0 &= \frac{(-1) \cdot 1234}{2} = -617. \end{aligned}$$

Comprobación.— En efecto, $12 \cdot 1851 + 34 \cdot (-617) = 22212 - 20978 = 1234$.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general —o sea, todas las soluciones— de (18.58), tomando como solución particular la anterior, es

$$\begin{aligned} x &= 1851 + k \cdot \frac{34}{2} = 1851 + 17k, \\ y &= -617 - k \cdot \frac{12}{2} = -617 - 6k \qquad (k \in \mathbb{Z}). \end{aligned}$$

Comprobación.— En efecto, $12 \cdot (1851 + 17k) + 34 \cdot (-617 - 6k) = 22212 + 204 - 20978 - 204 = 1234$.

V. *Cálculo de la solución de la cuestión en estudio.*

Calculemos, finalmente, la solución de la cuestión en estudio.

$$\begin{aligned} x > 0 &\to 1851 + 17k > 0 \to k > -\frac{1851}{17} = -108{,}88, \\ y > 0 &\to -617 - 6k > 0 \to k < -\frac{617}{6} = -102{,}83, \end{aligned}$$

de donde

$$-108{,}88 < k < -102{,}83,$$

por lo que los números $k \in \mathbb{Z}$ son

$$-108 \leq k \leq -103, \tag{18.61}$$

luego,

k	x = 1851 + 17k	y = -617 - 6k
-108	15	31
-107	32	25
-106	49	19
-105	66	13
-104	83	7
-103	100	1

Éstas son las seis posibilidades.

Solución.— Pudo comprar, bien 15 objetos de tipo A y 31 de tipo B, bien 32 de tipo A y 25 de tipo B, bien 49 de tipo A y 19 de tipo B, bien 66 de tipo A y 13 de tipo B, bien 83 de tipo A y 7 de tipo B, bien 100 de tipo A y 1 de tipo B. ■

Ejemplo 602

Considerando un número suficiente de monedas de 5, 10 y 20 céntimos, ¿de cuántas formas pueden 14 de tales monedas sumar 2 euros y cuáles son dichas formas? Resolvamos esta cuestión utilizando la teoría de las ecuaciones diofánticas.

[PEP 10.4.2019:5].

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Si x, y, z representan el número de monedas de 5, 10 y 20 céntimos, respectivamente, entonces, se tiene:

$$\begin{cases} 5x + 10y + 20z = 200, \\ x + y + z = 14, \end{cases}$$

que simplificando queda

$$\begin{cases} 5x + 10y + 20z = 200, \\ (-5)x + (-5)y + (-5)z = (-5)14 = -70, \end{cases}$$

Tenemos así la ecuación diofántica con dos variables,

$$5y + 15z = 130.$$

Estudiémosla.

II. *Demostración de que tiene al menos una solución.*

¿Tiene solución entera? Sí, por el teorema 18.107 (pág. 1047 de esta edición), pues $\text{mcd}(5, 15) = 5 \mid 130$.

III. *Cálculo de una solución particular.*

Coeficientes de Bézout: existen infinitos, ya que cualquier par $\langle s, t\rangle$ con $s = 1 - 3t$ con $t \in \mathbb{Z}$ es solución de la ecuación $5 = 5s + 15t$ (ecuación diofántica más sencilla que la original pero ecuación diofántica, a fin de cuentas); tomamos, por ejemplo, $s = -2$ y $t = 1$.

Una solución particular es:

$$y_0 = \frac{130 \cdot (-2)}{5} = -52,$$
$$z_0 = \frac{130 \cdot 1}{5} = 26.$$

Comprobación.— En efecto, $5 \cdot (-52) + 15 \cdot 26 = -260 + 390 = 130$.

IV. La solución general es:

$$y = -52 + \frac{k}{5} \cdot 15 = 3k - 52,$$
$$z = 26 + \frac{k}{5} \cdot (-5) = 26 - k,$$

siendo $k \in \mathbb{Z}$.

Comprobación.— En efecto, $5 \cdot (3k - 52) + 15 \cdot (26 - k) = 15k - 260 + 390 - 15k = 130$.

V. *Cálculo de la solución de la cuestión en estudio.*

Encontremos finalmente la solución particular para la cuestión en estudio. Para ello, intentemos acotar k. Como no puede usarse un número negativo de monedas, tenemos las cotas inferiores $x \geq 0$ e $y \geq 0$ y así,

$$0 \leq y \to 0 \leq 3k - 52 \to 52/3 = 17 + \frac{1}{3} \leq k,$$
$$0 \leq z \to 0 \leq 26 - k \to k \leq 26,$$

con $k \in \mathbb{Z}$, de donde $(18 \leq k \leq 26) \land k \in \mathbb{Z}$.

Se tienen entonces los siguientes valores para x, y, z según los valores de k:

$k =$	18	19	20	21	22	23	24	25	26
$y = 3k - 52 =$	2	5	8	11	14	17	20	23	26
$z = 26 - k =$	8	7	6	5	4	3	2	1	0
$x = 14 - (y + z) =$	4	2	0	-2	-4	-6	-8	-10	-12

Luego, existen tres soluciones: $\langle x, y, z\rangle = \langle 2, 5, 7\rangle$, $\langle x, y, z\rangle = \langle 4, 2, 8\rangle$ y $\langle x, y, z\rangle = \langle 0, 8, 6\rangle$.

Comprobación.— En efecto, $5 \cdot 5 + 15 \cdot 7 = 25 + 105 = 130$, $5 \cdot 2 + 15 \cdot 8 = 10 + 120 = 130$ y $5 \cdot 8 + 15 \cdot 6 = 40 + 90 = 130$.

Solución.— Existen tres formas en que 14 monedas de 5, 10 y 20 céntimos pueden sumar 2 euros: en las formas $\langle x, y, z\rangle = \langle 2, 5, 7\rangle$ y $\langle x, y, z\rangle = \langle 4, 2, 8\rangle$, utilizando monedas de los tres tipos, y en una tercera, $\langle x, y, z\rangle = \langle 0, 8, 6\rangle$, en la que sólo se usan monedas de 10 y 20 céntimos. ■

Ejemplo 603

Supongamos que el día D se ejecutaron once procesos en el computador C, que el tiempo total de la ejecución fue de 91 segundos y que los procesos fueron de dos tipos, A y B, que son tales que un proceso de tipo A tarda en ejecutarse siete segundos menos que uno de tipo B. En estas condiciones, ¿cuánto dura la ejecución de un proceso de tipo A y de uno de tipo B? y ¿cuántos procesos de cada tipo se ejecutaron el día D en el computador C?

[EFE 28.6.2023:6], [EFO 27.5.2025:6], [EFE 18.6.2025:6].

Resolución.— Sea a el número de procesos de tipo A y b el número de procesos de tipo B. Sea x (segundos) el tiempo que un proceso de tipo A tarda en ejecutarse (de donde un proceso de tipo B tarda $x + 7$ segundos). Tenemos lo que sigue.

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Lo expuesto en la totalidad del enunciado queda representado por el sistema de ecuaciones

$$a + b = 11,$$
$$ax + b(x + 7) = 91,$$

quedando esta segunda,

$$(a + b)x + 7b = 91,$$

de donde, sustituyendo la primera en esta última,

$$11x + 7b = 91. \tag{18.62}$$

Como buscamos soluciones enteras, tenemos así una ecuación diofántica con dos variables. Esta ecuación es irreducible en los enteros debido a que los números 11, 7 y 91 son primos entre sí.

II. *Demostración de que tiene al menos una solución.*

Por el algoritmo de EUCLIDES, el $\mathrm{mcd}(11, 7)$,

$$11 = 1 \cdot 7 + 4, \tag{18.63}$$
$$7 = 1 \cdot 4 + 3, \tag{18.64}$$
$$4 = 1 \cdot 3 + 1, \tag{18.65}$$
$$3 = 3 \cdot 1 + 0,$$

donde comprobamos que el resto anterior al nulo vale 1.

Por lo establecido en el teorema 18.107 (pág. 1047 de esta edición), esta ecuación diofántica tiene solución entera, ya que $\mathrm{mcd}(11, 7) = 1$ divide a 91.

III. *Cálculo de una solución particular.*

Coeficientes de BÉZOUT, existen infinitos, ya que cualquier par (s, t) con $s = \dfrac{1 - 7t}{11}$ con $t \in \mathbb{Z}$ es solución de la ecuación $11s + 7t = 1$.

De (18.65), (18.64) y (18.63), partiendo del máximo común divisor 1 y recorriendo el algoritmo de Euclides hacia atrás:

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (7 - 1 \cdot 4) \\ &= 2 \cdot 4 - 1 \cdot 7 \\ &= 2 \cdot (11 - 1 \cdot 7) - 1 \cdot 7 \\ &= 2 \cdot 11 + (-3) \cdot 7, \end{aligned}$$

por lo que unos coeficientes de Bézout s y t son 2 y -3, respectivamente, esto es, una solución —particular— de $11x + 7y = 1$ es $\langle x, y \rangle = \langle 2, -3 \rangle$.

Una solución particular de (18.62) es

$$\begin{aligned} x_0 &= \frac{91 \cdot 2}{1} = 182, \\ b_0 &= \frac{91 \cdot (-3)}{1} = -273. \end{aligned}$$

Comprobación.— En efecto, $11 \cdot 182 + 7 \cdot (-273) = 91$.

Observación.— $(182, -273)$ es una solución particular de $11x + 7b = 91$; no debe extrañarnos que $182 > 91$ ni que $-273 < 0$ pues aún no hemos introducido ninguna restricción semántica.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general de (18.62) es

$$\begin{aligned} x &= 182 + \frac{k}{1} \cdot 7 \\ &= 182 + 7k, \\ b &= -273 + \frac{k}{1} \cdot (-11) \\ &= -273 - 11k, \end{aligned}$$

siendo $k \in \mathbb{Z}$.

Comprobación.— En efecto, $11 \cdot (182 + 7k) + 7 \cdot (-273 - 11k) = 2002 + 77k - 1911 - 77k = 91$.

v. *Cálculo de la solución de la cuestión en estudio.*

Encontremos finalmente la solución particular para la cuestión en estudio. Para ello, intentemos acotar k. Tanto el tiempo x que tarda en ejecutarse un proceso de tipo A como el número b de procesos de tipo B deben ser positivos (ya que nos dicen que los procesos fueron de los dos tipos), por lo que

$$\begin{aligned} 0 < x &\to 0 < 182 + 7k \\ &\to -26 < k \\ &\to k \in \{-25, -24, -23, \dots\}, \\ 0 < b &\to 0 < -273 - 11k \\ &\to k < -\frac{273}{11} \\ &\to k \in \{\dots, -27, -26, -25\}, \end{aligned}$$

de donde

$$k = -25.$$

Se tiene entonces

$$\begin{aligned} x &= 182 + 7 \cdot (-25) = 7, \\ b &= -273 - 11 \cdot (-25) = 2, \end{aligned}$$

de donde

$$\begin{aligned} x + 7 &= 14, \\ a &= 11 - 2 = 9. \end{aligned}$$

Comprobación.— En efecto, $9 \cdot 7 + 2 \cdot (7 + 7) = 63 + 28 = 91$.

Solución.— Un proceso de tipo A tarda 7 segundos mientras que uno de tipo B se ejecuta en 14 segundos. En la ejecución del día D en el computador C intervinieron 9 procesos de tipo A y 2 procesos de tipo B. ■

Observación 18.20.1.— Hemos llegado a la ecuación (18.62) sustituyendo a por $11 - b$. Alternativamente,

- pudiésemos haber sustituido b por $11 - a$, en cuyo caso la ecuación (18.62) habría sido $11x - 7a = 14$;
- pudiésemos haber utilizado como segunda ecuación de partida $a(y - 7) + by = 91$, y
  - pudiésemos haber sustituido a por $11 - b$, en cuyo caso la ecuación (18.62) habría sido $11y + 7b = 168$;
  - pudiésemos haber sustituido b por $11 - a$, en cuyo caso la ecuación (18.62) habría sido $11y - 7a = 91$.

Observación 18.20.2.— Alternativamente, pudiésemos haber interpretado parcialmente la situación expuesta en el enunciado y tomado como ecuación diofántica $a + b = 11$. El procedimiento nos habría llevado a la solución particular $\langle a_0, b_0\rangle = \langle -11, 22\rangle$, ésta a la solución general $\langle a, b\rangle = \langle -11 + k, 22 - k\rangle$ ($k \in \mathbb{Z}$), de aquí y de $1 \leq a < 11$ y $1 \leq b < 11$ (nos dicen que se ejecutaron procesos de tipo A y de tipo B) a la acotación $12 \leq k < 22$ y de ésta a las posibles soluciones $\langle a, b\rangle$, a saber, $\langle 1, 10\rangle$, $\langle 2, 9\rangle$, $\langle 3, 8\rangle$, . . ., $\langle 8, 3\rangle$, $\langle 9, 2\rangle$, $\langle 10, 1\rangle$. A continuación tendríamos que comprobar cuáles de éstas hacen que $x = (91 - 7b)/(a + b) \in \mathbb{Z}$ (esta x proviene de $ax + b(x + 7) = 91$), esto es, que $(91 - 7b)/11 \in \mathbb{Z}$:

a	1	2	3	4	5	6	7	8	9	10
b	10	9	8	7	6	5	4	3	2	1
x	$21/11$	$28/11$	$35/11$	$42/11$	$49/11$	$56/11$	$63/11$	$70/11$	7	$84/11$

Como vemos, sólo el valor $\langle 9, 2\rangle$ para $\langle a, b\rangle$ hace que x (el tiempo que tarda un proceso de tipo A) sea un número entero.

Aún más, en este caso de aplicar la teoría de ecuaciones diofánticas a la ecuación $a + b = 11$, cabe preguntarnos por qué tomamos también como diofántica la ecuación $ax + b(x + 7) = 91$ con respecto a x. Así, si consideramos que los procesos no tienen por qué tardar en ejecutarse un número entero de segundos, todas las anteriores son soluciones:

a	1	2	3	4	5	6	7	8	9	10
b	10	9	8	7	6	5	4	3	2	1
x	$21/11$	$28/11$	$35/11$	$42/11$	$49/11$	$56/11$	$63/11$	$70/11$	7	$84/11$
y	$98/11$	$105/11$	$79/11$	$119/11$	$126/11$	$133/11$	$140/11$	$147/11$	14	$161/11$

Ésta es una tabla de soluciones por columnas. Por ejemplo, la columna encabezada por 7: un proceso de tipo A tarda $63/11$ segundos mientras que uno de tipo B se ejecuta en $140/11$ segundos;

en la ejecución del día D en el computador C intervinieron 7 procesos de tipo A y 4 procesos de tipo B.

Observación 18.20.3.— Veamos los apartados III), IV) y V) por teoría de congruencias. Expresemos la ecuación (18.62), esto es, $11x + 7b = 91$, como $7b \equiv 91 \pmod{11}$, la que como $\mathrm{mcd}(11, 7) = 1$, tiene solución única, que es $b \equiv 91 \cdot 7^{\varphi(11)-1} \pmod{11}$, esto es, $b \equiv 91 \cdot 7^{10-1} \pmod{11}$, es decir, $b \equiv 91 \cdot 7^9 \pmod{11}$, o sea, $b \equiv 2 \pmod{11}$ [¡esto requiere justificación! ✍], en definitiva, $x \in \{2, 13, 24, 35, 46, 57, 68, 79, 90, 101, 112, \ldots\}$. Como hay un total de once procesos, nos quedamos con el valor $b = 2$, esto es, hay dos procesos de tipo B en la ejecución del día D en el computador C. De aquí, $a = 11-2 = 9$, es decir, hay nueve procesos de tipo A en dicha ejecución en dicho computador.

Ahora, despejando b en (18.62), $b = (91 - 11x)/7$ y sustituyendo en $7b \equiv 91 \pmod{11}$, se tiene $7 \cdot (91-11x)/7 \equiv 91 \pmod{11}$, esto es, $(91-11x) \equiv 91 \pmod{11}$, es decir, $(91-11x) \equiv 91 \pmod{11}$, o sea, $x \equiv 0 \pmod{7}$ [¡esto requiere justificación! ✍], en definitiva, $x \in \{0, 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, \ldots\}$.

Pues bien, un proceso de tipo A no puede tardar en ejecutarse 0 segundos porque entonces un proceso de tipo B también tardaría cero segundos (el doble que un proceso de tipo A), pero entonces, once procesos de tipos A y B no podrían tardar 91 segundos (imaginando un redondeo a cero si los tiempos son menores que 0,5, el total de once procesos sería como algo menos de $11 \cdot 0{,}5 = 5{,}5$ segundos).

Así, un proceso de tipo A y un proceso de tipo B pueden tardar 7 y 14 segundos, respectivamente, o 14 y 28, o 21 y 42, o 28 y 56; 35 y 70 ya no pueden, porque $35 + 70 = 105 > 91$; 14 y 28 tampoco porque cualquier combinación lineal sería un número par y 91 no es par; 28 y 56 tampoco por el mismo motivo; 21 y 42 tampoco porque 91 no es múltiplo de 21; 7 y 14 sí, porque 91 es múltiplo de 7.

Observación 18.20.4.— Alternativamente, pudiésemos haber comenzado la observación anterior por $11x \equiv 91 \pmod{7}$, la que como $\mathrm{mcd}(11, 7) = 1$, tiene solución única, que es $x \equiv 91 \cdot 11^{\varphi(7)-1} \pmod{7}$, esto es, $x \equiv 91 \cdot 11^{6-1} \pmod{7}$, es decir, $x \equiv 91 \cdot 11^5 \pmod{7}$, o sea, $x \equiv 0 \pmod{7}$ [¡esto requiere justificación! ✍], en definitiva, $x \in \{0, 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, \ldots\}$.

Observación 18.20.5.— Si no la conoce, puede resultarle curiosa la *función* 91 *de* McCarthy[95].

Ejemplo 604

En los enteros, sea la sucesión definida así: comenzando en 0, cada término se obtiene del anterior sumándole o restándole 2 o 3 a este último. Demostremos que esta sucesión siempre alcanza el 4. A modo de ilustración, por ejemplo: $0 \overset{-2}{\longmapsto} -2 \overset{+3}{\longmapsto} 1 \overset{+3}{\longmapsto} 4$.

[EFE 25.6.2019:3].

[95] *Vid. v. gr.* https://en.wikipedia.org/wiki/McCarthy_91_function.

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Si x representa el número veces que se suma 2, y el número de veces que se suma 3, z el número de veces que se resta 2 y t el número de veces que se resta 3, entonces, se tiene lo que sigue.

La siguiente ecuación representa lo expuesto en el enunciado:

$$2(x - z) + 3(y - t) = 4. \tag{18.66}$$

Como se buscan soluciones enteras, se tiene así una ecuación diofántica, que reescribimos con dos variables; llamemos r a $x - z$ y s a $y - t$, entonces (18.66) es

$$2r + 3s = 4.$$

Esta ecuación es irreducible en los enteros —los números 2, 3 y 4 son (mutuamente) coprimos.

II. *Demostración de que tiene al menos una solución.*

¿Tiene solución entera? Sí, por el teorema 18.107 (pág. 1047 de esta edición), pues $\operatorname{mcd}(2, 3) = 1|4$.

III. *Cálculo de una solución particular.*

Como los coeficientes de Bézout son −1 y 1, una solución particular es

$$r_0 = \frac{4 \cdot (-1)}{1} = -4,$$
$$s_0 = \frac{4 \cdot 1}{1} = 4.$$

Comprobación.— En efecto, $2 \cdot (-4) + 3 \cdot 4 = -8 + 12 = 4$.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general es

$$\begin{aligned} r &= -4 + \frac{k}{1} \cdot 3 \\ &= -4 + 3k, \\ s &= 4 + \frac{k}{1} \cdot (-2) \\ &= 4 - 2k, \end{aligned}$$

siendo $k \in \mathbb{Z}$, ya que los valores de x, y, z y t son enteros no negativos (representan números de veces) y por tanto, $r, s \in \mathbb{Z}$.

Comprobación.— En efecto, $2 \cdot (-4 + 3k) + 3 \cdot (4 - 2k) = -8 + 6k + 12 - 6k = 4$.

v. *Cálculo de la solución de la cuestión en estudio.*

Como soluciones particulares de la cuestión en estudio se tienen los siguientes valores de r e s según los valores de $k \in \mathbb{Z}$:

$k =$	0	-1	1	-2	2	-3	...
$r = x - z = -4 + 3k =$	-4	-7	-1	-10	2	-13	...
$s = y - t = 4 - 2k =$	4	6	2	8	0	10	...

Por ejemplo, para $x - z = -4$ e $y - t = 4$, se tienen para (x, z, y, t) las infinitas combinaciones compuestas por un primer elemento de:

$x - z = -4$							
$x =$	0	1	2	3	4	5	...
$z =$	4	5	6	7	8	9	...

y un segundo de:

$y - t = 4$							
$y =$	4	5	6	7	8	9	...
$t =$	0	1	2	3	4	5	...

esto es,

(x, z, y, t)
$(0, 4, 4, 0)$
$(0, 4, 5, 1)$
$\vdots$
$(1, 5, 4, 0)$
$(1, 5, 5, 1)$
$\vdots$
$(2, 6, 4, 0)$
$(2, 6, 5, 1)$
$\vdots$



Observación 18.20.6.— La solución dada a modo de ilustración en el enunciado del ejemplo, $0 \overset{-2}{\longmapsto} -2 \overset{+3}{\longmapsto} 1 \overset{+3}{\longmapsto} 4$, corresponde a $k = 1$, $r = -1$, $s = 2$, $x = 0$, $z = 1$, $y = 2$, $t = 1$.

Conjetura de Collatz

Propuesta por Lothar Collatz, en 1937: comenzando en cualquier entero positivo, cada término se obtiene del anterior dividiéndolo entre dos si es par o multiplicándolo por 3 y sumándole 1 si es impar (por cierto, *cfr. supra* actividad 12.4 [pág. 712 de esta edición]). La conjetura de Collatz* afirma que la sucesión así formada siempre

alcanza el 1. Nadie ni nada lo ha demostrado aún. A modo de ilustración, por ejemplo: $23 \xmapsto{\cdot 3+1} 70 \xmapsto{/2} 35 \xmapsto{\cdot 3+1} 106 \xmapsto{/2} 53 \xmapsto{\cdot 3+1} 160 \xmapsto{/2} 80 \xmapsto{/2} 40 \xmapsto{/2} 20 \xmapsto{/2} 10 \xmapsto{/2} 5 \xmapsto{\cdot 3+1} 16 \xmapsto{/2} 8 \xmapsto{/2} 4 \xmapsto{/2} 2 \xmapsto{/2} 1$.[†]

Paul Erdős[‡] afirmó en 1983 que «las matemáticas aún no están lo suficientemente maduras para estas preguntas», opinión compartida por Jeff Lagarias en 2010: «éste es un problema extraordinariamente difícil, completamente fuera del alcance de las matemáticas actuales»[§]. Terence Tao explora la vía estadística; él demuestra en 2019 que casi todos los números (en el sentido de la densidad logarítmica) alcanzan valores mínimos casi acotados (y, por lo tanto, «próximos» a uno)[¶].

Vid. etiam actividad A.9 (pág. 1430 de esta edición).

[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/Collatz_conjecture; https://www.dcode.fr/collatz-conjecture.

[†] *Vid. v. gr.* https://rosettacode.org/wiki/Hailstone_sequence para conocer implementaciones en diferentes lenguajes de programación de la generación de la sucesión de números de Collatz para un número determinado.

[‡] *Vid. v. gr.* https://en.wikipedia.org/wiki/Paul_Erd%C5%91s.

[§] Vía Terence Tao, https://terrytao.wordpress.com/wp-content/uploads/2020/02/collatz.pdf y https://terrytao.wordpress.com/wp-content/uploads/2020/04/collatz-1.pdf.

[¶] *Vid.* https://terrytao.wordpress.com/2019/09/10/almost-all-collatz-orbits-attain-almost-bounded-values/ y https://terrytao.wordpress.com/wp-content/uploads/2020/04/collatz-1.pdf.

Actividad 18.36

En base diez, para cualquier número n de cuatro cifras con al menos dos cifras distintas, siendo n_y el número obtenido al reordenar las cifras de n de mayor a menor y n_o el obtenido al reordenar las cifras de n de menor a mayor, y restamos $n_y - n_o$ y a este número le volvemos a aplicar el proceso, y así reiteradamente, llegaremos al número 6174, la *constante de* Kaprekar[*]. Investiguemos cuál es su porqué, qué sucede para otros números de cifras y en otros sistemas de numeración. (Un ejemplo en base diez: $2026 \xmapsto{6220-0226} 5994 \xmapsto{9954-4599} 5355 \xmapsto{5553-3555} 1998 \xmapsto{9981-1899} 8082 \xmapsto{8820-0288} 8532 \xmapsto{8532-2358} 6174$).

[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/D._R._Kaprekar.

Ejemplo 605

Una empresa gastó 100 000 euros en 100 dispositivos electrónicos, algunos de última generación y máximas prestaciones. Compró teléfonos inteligentes a 50 euros, tabletas a 1000 y portátiles a 5000. ¿Cuántos dispositivos compró de cada clase? Hallemos la solución utilizando: 0.º, la teoría de ecuaciones diofánticas, y 1.º, la teoría de ecuaciones en congruencias.

[SEL 8:1]. *Cfr.* González [153]: ejemplo 12.8 (pág. 353).

Resolución.— Veamos:

0.°, Por la teoría de ecuaciones diofánticas:

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Traducida la información del enunciado a un sistema de ecuaciones lineales y simplificado éste,

$$\begin{cases} x+y+z=100 \\ 50x+1000y+5000z=100\,000 \end{cases} \to \begin{cases} x+y+z=100 \\ x+20y+100z=2000 \end{cases}$$
$$\to \begin{cases} x+y+z=100 \\ x+y+z+19y+99z=2000 \end{cases}$$
$$\to 100+19y+99z=2000$$
$$\to 99z+19y=1900$$

II. *Demostración de que tiene al menos una solución.*

Por el teorema 18.107 (pág. 1047 de esta edición), una ecuación diofántica lineal $ax+by=c$ tiene solución precisamente si $\operatorname{mcd}(a,b)\,|\,c$.

III. *Cálculo de una solución particular.*

Una solución particular de la ecuación es $\langle x_0, y_0\rangle = \langle cs/d, ct/d\rangle$ donde $d=\operatorname{mcd}(a,b)$ y s y t son los coeficientes de a y b en la combinación lineal igual a d (identidad de Bèzout).

El siguiente cuadro muestra la utilización del algoritmo de Euclides extendido para el caso que nos ocupa. La computación se detiene cuando el resto es cero (en color rojo). El resto anterior, 1 (en color rojo), es el máximo común divisor. Los coeficientes de Bézout s y t son 5 y −26 (en color magenta). Los números en cian, −19 y 99, sin considerar el signo, son los cocientes de los originales entre el máximo común divisor.

i	q_{i-1}	r_i	s_i	t_i
0		99	1	0
1		19	0	1
2	99 / 19 = 5	99 - 5 · 19 = 4	1 - 5 · 0 = 1	0 - 5 · 1 = -5
3	19 / 4 = 4	19 - 4 · 4 = 3	0 - 4 · 1 = -4	1 - 4 · (-5) = 21
4	4 / 3 = 1	4 - 1 · 3 = 1	1 - 1 · (-4) = 5	-5 - 1 · 21 = -26
5	3 / 1 = 3	3 - 3 · 1 = 0	-4 - 3 · 5 = -19	21 - 3 · (-26) = 99

Por lo tanto, una solución particular es

$$z_0 = \frac{1900 \cdot 5}{1} = 9500,$$
$$y_0 = \frac{1900 \cdot (-26)}{1} = -49\,400,$$

Comprobación.— En efecto, $99 \cdot 9500 + 19 \cdot (-49\,400) = 940\,500 - 938\,600 = 1900$.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general de dicha ecuación es

$$\{\langle x, y\rangle : k \in \mathbb{Z}\},$$

con

$$x = x_0 + \frac{k \cdot b}{d},$$
$$y = y_0 - \frac{k \cdot a}{d},$$

esto es,

$$z = 9500 + \frac{k \cdot 19}{1},$$
$$y = -49\,400 - \frac{k \cdot 99}{1},$$

con $k \in \mathbb{Z}$.

Comprobación.— En efecto, $99 \cdot (9500 + 19k) + 19 \cdot (-49\,400 - 99k) = 940\,500 + 1881k - 938\,600 - 1881k = 1900$.

V. *Cálculo de la solución de la cuestión en estudio.*

Ahora bien, ¿cuántos dispositivos compró de cada clase, sabiendo que compró al menos uno de cada clase? Veamos. Sabemos que $z > 0$ y que $y > 0$. Por tanto, $9500 + 19k > 0$ y $-49400 - 99k > 0$, de donde $-500 < k$ y $k < -498,9$. Como $k \in \mathbb{Z}$, $k = -499$. Sustituyendo, obtenemos $z = 19$, $y = 1$ y $x = 100 - 1 - 19 = 80$.

Comprobación.— En efecto, $99 \cdot 19 + 19 \cdot 1 = 1881 + 19 = 1900$.

Solución.— [Por la teoría de las ecuaciones diofánticas]. Esta empresa compró ochenta teléfonos, una tableta y diecinueve portátiles. □

1.°, Por la teoría de ecuaciones en congruencias.

Vista como una ecuación en congruencias, puede ser $99z \equiv 1900 \pmod{19}$, o su equivalente, $99z \equiv 0 \pmod{19}$.

Como mcd $(99, 19) = 1$, este camino nos lleva a que son posibles soluciones todos los múltiplos positivos de 19 menores que 100, esto es, $z \in \{19, 38, 57, 76, 95\}$.

Probemos otro camino. La ecuación diofántica $99z + 19y = 1900$ también tiene otra vista como ecuación en congruencias, a saber, $19y \equiv 1900 \pmod{99}$, o su equivalente, $19y \equiv 19 \pmod{99}$.

Como mcd $(99, 19) = 1$, esta ecuación tiene una solución única $\pmod{99}$, que es $y \equiv 19 \cdot 19^{\phi(99)-1} \pmod{99}$, esto es, $y \equiv 19^{60} \pmod{99}$.

Explorando los residuos potenciales, encontramos que $19^{10} \equiv 1 \pmod{99}$ de donde, multiplicando esta congruencia seis veces, miembro a miembro, obtenemos que $19^{60} \equiv 1 \pmod{99}$ y por ser transitiva la relación de congruencia, que $y \equiv 1 \pmod{99}$.

Es decir, $y = 1$ (ya que $y < 100$).

Como $99z + 19y = 1900$, obtenemos que $z = 19$.

Finalmente, de $x + y + z = 100$, tenemos que $x = 80$.

Comprobación.— En efecto, $99 \cdot 19 + 19 \cdot 1 = 19 \cdot (99 + 1) = 1900$.

Solución.— [Por la teoría de las ecuaciones en congruencias]. Esta empresa compró ochenta teléfonos, una tableta y diecinueve portátiles. ■

Ejemplo 606

¿Cómo pudiésemos distribuir 100 litros de agua en un total de 40 recipientes varios, de 1, 4 y 12 litros?

[EFO 24.5.2018:3], [SEL 8:4]. *Cfr.* Perelmán [208]: § 4.3 Compra de sellos de correos (págs. 158–160).

Resolución.—

I. *Propuesta razonada de una ecuación diofántica que modeliza la situación expuesta.*

Representando por x, y, z, los números de recipientes usados de 1, 4 y 12 litros, respectivamente, el enunciado se traduce en las ecuaciones $x + y + z = 40$ y $x + 4y + 12z = 100$.

Restando de la segunda ecuación la primera, tenemos la ecuación diofántica $3y + 11z = 60$.

II. *Demostración de que tiene al menos una solución.*

Como mcd$(3, 11) = 1 \mid 60$, esta ecuación diofántica tiene solución entera [por lo establecido en el teorema 18.107 (pág. 1047 de esta edición)].

III. *Cálculo de una solución particular.*

Por simple inspección, como $1 = 4 \cdot 3 + (-1) \cdot 11$, los coeficientes de BÉZOUT son $s = 4$ y $t = -1$. Una solución particular es $y_0 = 4 \cdot 60/1 = 240$, $z_0 = (-1) \cdot 60/1 = -60$.

Comprobación.— En efecto, $3 \cdot 240 + 11 \cdot (-60) = 720 - 660 = 60$.

IV. *Cálculo de la solución general a partir de la particular anterior.*

La solución general es $y = 240 + 11k$, $z = -60 - 3k$, con $k \in \mathbb{Z}$.

Comprobación.— En efecto, $3 \cdot (240 + 11k) + 11 \cdot (-60 - 3k) = 720 + 33k - 660 - 33k = 60$.

V. *Cálculo de la solución de la cuestión en estudio.*

Suponiendo que en la solución interviene al menos un recipiente de cada tipo, tenemos que $0 < y, z \leq 40 - (1 + 1) = 38$.

Sustituyendo en estas últimas la solución general encontrada, tenemos, por un lado, que $0 < 240 + 11k \leq 38$, de donde $-240/11 < k \leq -202/11$, por lo que $-21,82 < k \leq -18,36$ y, por tanto, $k \in \{-21, -20, -19\}$, y por otro lado, que $0 < -60 - 3k \leq 38$, de donde $60/3 < -k \leq 98/3$, por lo que $-98/3 \leq k < -60/3$, esto es, $-32,67 \leq k < -20$ y, por tanto, $k \in \{-32, \dots, -22, -21\}$. Como $k \in \{-21, -20, -19\} \cap \{-32, \dots, -22, -21\}$, obtenemos que $k = -21$. Sustituyendo en la solución general, $y = 240 + 11 \cdot (-21) = 9$ y $z = -60 - 3 \cdot (-21) = 3$, por lo que $x = 40 - (9 + 3) = 28$.

Comprobación.— En efecto, $3 \cdot 9 + 11 \cdot 3 = 27 + 33 = 60$.

Solución.— Suponiendo que al menos debe llenarse un recipiente de cada tipo, se emplean veinte recipientes de un litro, nueve de cuatro litros y tres de doce litros. Claro que si no lo supusiésemos, cabría otra solución: veinte de un litro, veinte de cuatro litros y cero de doce litros. ¡Comprobémoslo! (✍). ■

§ 18.21 Propuesta de más actividades

Actividad 18.37

Demostremos que $\log_2 3 \notin \mathbb{Q}$.

Con miras a su resolución.— Sea $r = \log_2 3$. Entonces, por definición de logaritmo, $2^r = 3$. Razonemos por reducción al absurdo: i $r \in \mathbb{Q}$, entonces $\exists p \in \mathbb{Z}$, $q \in \mathbb{Z}^+$ tal que $r = p/q$, de donde $p = q \log_2 3$, por lo que $p = \log 23^q$, y, por tanto, $2^p = 3^q$; sin embargo, esto no es cierto: no existen $p \in \mathbb{Z}$ y $q \in \mathbb{Z}^+$ tales que $2^p = 3^q$ —*vid.* ejemplo 413 (pág. 807 de esta edición)—.

Actividad 18.38

¿Es cierto que para tres números enteros cualesquiera x, y, z se satisface que si $x < y$, entonces $|x - z| < |y - z|$?

Con miras a su resolución.— No, por ejemplo, si $x = 0$, $y = 1$, $z = 2$, entonces $|x - z| = |0 - 2| = 2 \not< 1 = |1 - 2| = |y - z|$ (aunque sí es cierto $\forall x, y, z \in \mathbb{Z}$ que $x < y \to x - z < y - z$).

Actividad 18.39

La sexta parte del producto de tres números naturales consecutivos, ¿es un número natural?

Sugerencia.— Inducción débil sobre n.

Actividad 18.40

Demostremos que $\forall n \in \mathbb{Z}$, n es par $\leftrightarrow n^2$ es par (lo cual equivale a demostrar que $\forall n \in \mathbb{Z}$, n es impar $\leftrightarrow n^2$ es impar).

Actividad 18.41

Sea una variable de tipo palabra de n bits etiquetados de 1 a n. Inicializamos dicha variable con todos los bits en estado 1. Un dispositivo puede actuar de n formas distintas en la palabra: la forma 1 cambia el estado de todos los bits; la forma 2 cambia el estado de los bits de dos en dos comenzando por el bit 2, y así sucesivamente, esto es, en general, la forma k cambia el estado de los bits de k en k comenzando por el bit k. Si dicho dispositivo ejecuta secuencialmente las formas de actuar $1, 2, \ldots, n$, entonces:

0. ¿qué número de veces cambia de estado el bit r?;
1. ¿qué bits quedarán en un estado distinto de su estado inicial y por qué?

ⓘ Para resolver esta cuestión, debemos utilizar un razonamiento de teoría de números basado en lo estudiado (si utilizamos un criterio de divisibilidad, debemos demostrarlo).

[PEP 14.4.2023:5]. *Cfr.* García, López y Puigjaner [154]: problema 1.79 (pág. 61).

Actividad 18.42

Resolvamos en $\mathbb{Z}^+$ el sistema de ecuaciones:

$$\begin{cases} x + y = 396 \\ \text{mcd}(x, y) = 33 \end{cases}$$

[SEL 6:2]. *Cfr.* Prada y Rodríguez [205]: ejercicio 4.1.3 (págs. 33–34).

. . . .

Las siguientes cuatro cuestiones, por orden, son los ejercicios 7.1 (pág. 137), 7.12 (pág. 143), 7.10 (pág. 142) y 7.27 (pág. 149) del libro [197] Máximo ANZOLA GONZÁLEZ y José Ramón CARUNCHO CASTRO. *Problemas de álgebra. Tomo 2: Anillos - Polinomios - Ecuaciones.* Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1982. ©TDR.

. . . .

Actividad 18.43

Hallemos $m, n \in \mathbb{Z}^+$, con $\operatorname{mcm}(m, n) = 33$ y tales que la suma de sus cuadrados sea 1098.

[SEL 6:3].

Actividad 18.44

Hallemos $m, n \in \mathbb{Z}^+$ tales que $\operatorname{mcd}(m, n) = 12$ y $\operatorname{mcm}(m, n) = 396$.

[SEL 6:5].

Actividad 18.45

Hallemos $m, n \in \mathbb{Z}^+$ tales que m tiene 33 divisores, n tiene 22 divisores y $\operatorname{mcd}(m, n) = 245$.

[SEL 6:6].

Actividad 18.46

Hallemos el menor $n \in \mathbb{Z}^+$ que satisface $\begin{cases} n \text{ mód } 2 = 1 \\ n \text{ mód } 3 = 2 \\ n \text{ mód } 4 = 3 \\ n \text{ mód } 5 = 4 \\ n \text{ mód } 6 = 5 \\ n \text{ mód } 7 = 6 \end{cases}$

[SEL 6:8].

. . . .

Las siguientes son sobre congruencias.

. . . .

Actividad 18.47

Demostremos que $\forall n \in \mathbb{N}$, $23^n - 1$ es divisible por 11.

Actividad 18.48

¿Existe algún $m \in \mathbb{Z}^+$ tal que $a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$ es congruente con $a_k + a_{k-1} + \cdots + a_1 + a_0$, módulo m, sea cual sea $k \in \mathbb{N}$?

Las siguientes son sobre criterios de divisibilidad.

Actividad 18.49

Se nos requiere para:

0. a. utilizando el criterio general de divisibilidad, hallar el criterio de divisibilidad por dos en el sistema de numeración heptal* (base 7);
   b. utilizando el criterio de divisibilidad hallado en el apartado anterior, averiguar si el número heptal $12321_{(7}$ es divisible por dos;
1. finalmente, si no lo es, usar el criterio de divisibilidad hallado para sustituir la cifra heptal 3 por otra cifra heptal x tal que el número heptal $12x21_{(7}$ sea divisible por dos.

[EFE 24.5.2018:4] (tipo test).

* El *sistema de numeración heptal* (o, sinónimamente, *septinario* o *septimal*) tiene siete como su base (*vid. v. gr.* https://en.wikipedia.org/wiki/Septenary).

Actividad 18.50

Se nos requiere para:

0. a. utilizando el criterio general de divisibilidad, hallar el criterio de divisibilidad por seis en el sistema de numeración heptal (base 7);
   b. responder a la pregunta: ¿es divisible por seis el número heptal $1234321_{(7}$?;
1. finalmente, si no lo es, para sustituir la cifra heptal 4 por otra cifra heptal x tal que el número heptal $123x321_{(7}$ sea divisible por seis.

[AIC 10.4.2018:6A], [AIC 10.4.2018:6B] (divisibilidad por 3).

Las siguientes, sobre ecuaciones diofánticas.

Actividad 18.51

Un párrafo consta de 100 palabras, con un total de 323 letras. Estas palabras tienen dos, tres o cuatro letras. ¿Cuántas palabras hay de cada clase?

Con miras a su resolución.— De $x + y + z = 100$ y $2x + 3y + 4z = 323$, obtenemos $2x + y = 77$, de cuya solución, $x = 1$ e $y = 75$, se sigue $x = 1 + t$, $y = 75 - 2t$, $z = 24 + t$, de donde, como $x, y, z \in \mathbb{Z}^+$, $-1 < t < 75/2$, por lo que, si $t = -1$, $z = 23$, y si $t = 37$, $z = 61$, en definitiva, $z \in [23, 61]$.

Actividad 18.52

Dos personas llevaban un cesto de huevos. Un caballo que pasó a su lado hizo un extraño y les asustó, cayéndose el cesto y rompiéndose todos los huevos. La persona al cargo del caballo, queriendo pagarles su pérdida, les preguntó cuántos huevos llevaban. Ellas recordaban que eran entre 100 y 110 y que al contarlos en manos de tres sobraban dos y en manos de cuatro, sobraban tres. Calculemos el número de huevos utilizando la teoría de las ecuaciones diofánticas.

[EFO 1.6.2017:3a]. *Cfr.* GONZÁLEZ [153]: ejemplo 12.6 (pág. 351).

Actividad 18.53

Le pedimos a una persona que haga mentalmente las multiplicaciones de su día y mes de nacimiento por 12 y 31, respectivamente; a continuación, nos dirá el resultado de la suma de ambas multiplicaciones. De vuelta, le decimos qué día y mes nació. ¿Cómo?

[SEL 8:2]. *Cfr.* PERELMÁN [208]: § 4.5 Adivinar el día de nacimiento (págs. 162–165).

Actividad 18.54

Hurgando por aquí y allá, recogimos 17 monedas de 2 euros. Con ellas, fuimos a una tienda a comprar un objeto de valor 11 euros. La caja estaba ya cerrada y sólo tenían 4 billetes de 5 euros para darnos el cambio. ¿Pudimos comprar el objeto por su precio exacto?

[AIC 10.4.2018:5B], [SEL 8:3]. *Cfr.* PERELMÁN [208]: § 4.1 Compra de una bufanda (págs. 149–155).

Con miras a su resolución.— Designando x el número de monedas de dos euros e y el número de billetes de cinco euros, la ecuación diofántica es $2x - 5y = 11$ sujeta a las condiciones $0 < x \leq 17$ y $0 < y \leq 4$.

Actividad 18.55

Hemos comprado entre 50 y 100 objetos a 17 euros cada uno. De ellos, hemos vendido algunos a 35 euros cada uno, obteniendo un beneficio de 123 euros. ¿Cuántos nos quedan por vender?

[AIC 10.4.2018:5A], [SEL 8:5]. *Cfr.* OLIVÁN [209]: problema 1 (pág. 61).

Con miras a su resolución.— Designando x el número de objetos comprados e y el número de objetos vendidos, la ecuación diofántica es $35y - 17x = 123$ sujeta a la condición $50 < x < 100$.

Actividad 18.56

Hecha una auditoría, se ha descubierto que se compraron 12 objetos de dos tipos, A y B, por un total de 1200 euros, y que cada objeto de tipo A costó 30 euros más que cada uno de tipo B, y que se compró el mínimo posible de estos últimos. Sin embargo, no figura cuántos se compraron de cada tipo. ¿Pudiésemos saberlo?

[SEL 8:6]. *Cfr.* González [153]: ejemplo 12.3 (pág. 347).

Con miras a su resolución.— Designando x el número de objetos de tipo A comprados e y el coste de cada objeto de tipo B comprado, la ecuación diofántica es $x(y+30)+y(12-x)=1200$, ecuación que operando se transforma en una lineal de grado uno de dos variables.

Actividad 18.57

En un sistema informático determinado, procesar una consulta de tipo I supone un coste computacional de 700 ucb (unidades de coste de bit), una de tipo II un coste de 550 ucb y procesar una de tipo III un coste de 390 ucb. Si dicho sistema ha procesado 69 consultas con un coste computacional total de 32 740 ucb, ¿cuántas consultas puede haber habido de cada tipo?

[PEP 14.4.2023:6]. *Cfr.* García, López y Puigjaner [154]: problema 1.72 (pág. 56).

Actividad 18.58

Un robot es capaz de dar saltos de exactamente 1 m (salto corto) tanto hacia adelante como hacia atrás y de exactamente 2 m (salto largo) sólo hacia adelante, todos perfectamente alineados en horizontal. Si se desconoce en todo momento qué tipo de salto va a dar el robot, ¿puede éste recorrer exactamente 23 metros en línea recta en exactamente 15 saltos?

[EFEC 25.6.2019:3].

Con miras a su resolución.— Designando x el número de saltos cortos hacia adelante, y el número de saltos largos y z el número de saltos cortos hacia atrás, se trata de resolver el sistema de ecuaciones diofánticas lineales $\{x+2y-z=23; x+y+z=15\}$.

Siguen algunas cuestiones de *matemagia*[96], sencillitas, más divertimentos que otra cosa, pero no dudemos que siempre se aprende; pudiésemos decir que son de adivinación y mentalismo.

[96] La matemagia es un capítulo de la Matemática Recreativa (https://en.wikipedia.org/wiki/Recreational_mathematics), rama de la matemática de la que se han publicado muchas obras a lo largo del tiempo —a modo de ejemplo, *Ludi mathematici* de Leon Battista Alberti—. Pudiésemos aprender sobre matemagia de la mano de Carlos Vinuesa en Matemagia «básica» (https://gaceta.rsme.es/abrir.php?id=983) y de Adrián Paenza (http://cms.dm.uba.ar/material/paenza). *Vid. et. supra* ejemplo 18.26 (pág. 1031 de esta edición), ejemplo 521 (pág. 956 de esta edición) y Matemagia: el mejor truco de cartas (pág. 1190 de esta edición).

Actividad 18.59

Tres personas acaban de comer juntas en un restaurante. La comida les ha costado 10 euros a cada una. Pagan, pues, 30 euros al camarero, quien los entrega en caja, donde la propietaria le informa de que esas tres personas son buenas clientes y le dice que les devuelva 5 euros. El camarero, en vista de que no le dieron propina, les entrega sólo 3 euros, uno a cada una, guardándose en su bolsillo los otros 2. Resulta, pues, ahora, que las tres personas han pagado 9 euros cada una, o sea, 27 euros en total, que más los 2 que se guardó el camarero suman 29. ¿Dónde está el euro que falta?[97]

Cfr. Ciuró [210], Serie V, Problemas de ilusionismo, Otro (pág. 132).

Actividad 18.60

Pensemos un número de tres cifras; escribámoslo repetido, lo que nos da un número de seis cifras; dividamos éste sucesivamente por los primos siete, once y trece, esto es, el número de seis cifras por siete; el resultado por once, y el nuevo resultado, por trece. ¿Por qué obtenemos siempre el número pensado? ¿Ocurrirá con otros primos? ¿Tendrán que ser éstos primos consecutivos?

Con miras a su resolución.— Porque $xyzxyz = xyz \cdot 1001$, y $1001 = 7 \cdot 11 \cdot 13$.

Actividad 18.61

Retirar una o cuatro cartas de un grupo de veinte: tres jugadores—. Juegan tres personas, por turnos, retirando una o cuatro cartas en cada turno. Gana el juego quien retire la última carta. Si jugásemos a este juego y éste comenzase con veinte cartas, procuraríamos jugar en segundo lugar, ¿por qué?

Cfr. Meirovitz y Jacobs [211], 4. Juegos de estrategia conflictiva. EC 6-1 (pág. 178).

Actividad 18.62

Colocamos arbitrariamente sobre una mesa un número de monedas en las que sea fácilmente identificables su cara y su cruz. Nos volvemos de espalda y pedimos a alguien que dé vuelta a cuantas monedas quiera cuantas veces quiera de una en una diciendo en voz alta «vuelta» cada vez que lo haga y que después tape una moneda. Nos giramos de cara y adivinamos si la moneda tapada presenta bocarriba su cara o su cruz. ¿Por qué conseguimos adivinarlo?

Cfr. Ciuró [210], Serie I, Juegos de adivinación y mentalismo, ¿Cara o cruz? (pág. 13).

[97] Puro ilusionismo, ¿a que sí? Ésta es la primera cuestión de matemagia que aprendí y que recuerdo con mucho cariño porque también fue la primera que me enseñó mi madre.

Actividad 18.63

Escribamos un número decimal cualquiera de tres cifras que no sea capicúa, que no tenga las cifras iguales y que su primera cifra sea mayor que la última. Restémosle el número formado por sus cifras invertidas de lugar —si era abc, restémosle cba—. Sumemos al número resultante el número formado por sus cifras invertidas de lugar. Dará siempre como resultado 1089. ¿Verdad?

Cfr. Ciuró [210], Serie V, Problemas de ilusionismo, Otro (pág. 132).

Sigue un pequeño `proyecto de computación`.

Actividad 18.64

Con ayuda de un computador, demostremos que el número 23:

0. es el menor primo con un número primo de dígitos primos cuya suma es un número primo;
1. es el menor primo para el que la suma de los cuadrados de sus dígitos es un primo impar;
2. es el menor primo que es igual a la suma de tres primos distintos de dos formas diferentes;
3. el menor primo de la forma $p^p - q^q$ donde p y q son primos;
4. es el mayor entero que no es la suma de potencias distintas.

Observación 18.21.0.— Por cierto, $23 = 0^5 + 1^4 + 2^3 + 3^2 + 4^1 + 5^0$. Por otro lado, la sucesión constante 23 está catalogada en la OEIS como la sucesión A010862 (https://oeis.org/A010862). Para saber más, pudiésemos consultar, por ejemplo, https://en.wikipedia.org/wiki/23_(number).

Actividad 18.65

¿Pudiese sernos de utilidad haber estudiado teoría de números para solucionar el problema de las garrafas que se plantea en esta secuencia de la película *La jungla de cristal 3: la venganza*: https://www.youtube.com/watch?v=2vdF6NASMiE?

Actividad 18.66

Aprendamos a calcular la cifra de las unidades en potencias vía su periodicidad.*

* Como punto de partida, *vid. v. gr.* https://www.geeksforgeeks.org/maths/number-system-cyclicity-of-numbers/.

Actividad 18.67

Resolvamos el *problema del mono y los cocos* (*vid. v. gr.* http://recursostic.educacion.es/descartes/web/materiales_didacticos/coco_y_monos_ec_diofanticas/enunciado.htm y https://en.wikipedia.org/wiki/The_monkey_and_the_coconuts).

§ 18.22 Muestra de ejemplos finales

Ejemplo 607

¿Cuál es el menor número decimal n tal que su producto por 11 —esto es, $11n$— se escribe en base 13 (sistema de numeración tridecimal) sólo con cifras 6, esto es, $66\ldots6_{(13}$?

[EFO 12.6.2020:2a (p.h.e.c.)].

Resolución.— Según este enunciado, $11n$ en base 13 es

$$\begin{aligned}11n &= 6+6\cdot 13+6\cdot 13^2+\cdots+6\cdot 13^{k-1}\\ &= 6\cdot\left(1+13+13^2+\cdots+13^{k-1}\right)\\ &= 6\cdot\left(\frac{13^{k-1}\cdot 13-1}{13-1}\right)\\ &= \frac{1}{2}\left(13^k-1\right)\end{aligned}$$

(hemos podido sumar por ser la suma parcial de los primeros k términos de una progresión geométrica de razón 13, primer término 1 y último término 13^{k-1})[98], de donde, $\left(13^k-1\right)$ es divisible por 11 (por no serlo $1/2$), esto es,

$$13^k-1\equiv 0 \pmod{11},$$

es decir,

$$13^k\equiv 1 \pmod{11}. \tag{18.67}$$

Como

$$13\equiv 2 \pmod{11},$$

por la propiedad de potencia,

$$13^k\equiv 2^k \pmod{11},$$

que por simetría de $\equiv \pmod{11}$ (es una relación de equivalencia), es

$$2^k\equiv 13^k \pmod{11}. \tag{18.68}$$

[98] La suma parcial $a_0+r\cdot a_1+r^2\cdot a_2+\cdots+r^n\cdot a_n$ es $\dfrac{r\cdot a_n-a_0}{r-1}$.

De 18.68 y 18.67, por transitiva de $\equiv \pmod{11}$:

$$2^k \equiv 1 \pmod{11}.$$

Averigüemos cuál es el menor $k > 0$ tal que $2^k \equiv 1 \pmod{11}$: $2^1 \equiv 2 \pmod{11}$, $2^2 \equiv 4 \pmod{11}$, $2^3 \equiv 8 \pmod{11}$, $2^4 \equiv 5 \pmod{11}$, $2^5 \equiv 10 \pmod{11}$, $2^6 \equiv 9 \pmod{11}$, $2^7 \equiv 7 \pmod{11}$, $2^8 \equiv 3 \pmod{11}$, $2^9 \equiv 6 \pmod{11}$, $2^{10} \equiv 1 \pmod{11}$, resultando que dicho menor k es 10.

De aquí,

$$\begin{aligned} 11n &= \frac{1}{2}\left(13^{10} - 1\right) \\ &= \frac{1}{2}\left(137858491849 - 1\right) \\ &= 68\,929\,245\,924, \end{aligned}$$

de donde

$$\begin{aligned} n &= \frac{68\,929\,245\,924}{11} \\ &= 6\,266\,295\,084. \end{aligned}$$

Solución.— El menor número decimal tal que su producto por 11 se escribe en base 13 sólo con cifras 6 es 6 266 295 084. ■

Ejemplo 608

Consideremos una red en línea (en bus) de 18 computadores, de los que 17 tienen igual potencia de cómputo y uno, Litty, el último de la red, tiene menor potencia. Se trata de repartir n tareas entre todos ellos. La primera vez se decide repartir las tareas por igual entre los 17 y las que sobren para Litty, recibiendo éste 3 tareas. Tras un fallo generalizado, no puede contarse ya con 6 de los de mayor potencia; entonces, se vuelven a repartir las tareas por igual entre los de mayor potencia, recibiendo Litty 4. De nuevo se produce otro fallo generalizado, quedando sólo 6 de los computadores de mayor potencia y Litty. Se hace un nuevo reparto, de nuevo por igual entre los de mayor potencia, recibiendo Litty 5 tareas. La pregunta es, ¿cuál es el mínimo número n de tareas que se ha estado repartiendo siempre? Resolvámoslo: 0.º, por la teoría de congruencias, y 1.º, por la teoría de las ecuaciones diofánticas.

[EFO 12.6.2020:2b (p.h.e.c.)].

Resolución.— El enunciado se traduce en el sistema de congruencias lineales

$$n \equiv 3 \pmod{17}, \tag{18.69}$$
$$n \equiv 4 \pmod{11}, \tag{18.70}$$
$$n \equiv 5 \pmod{6}, \tag{18.71}$$

cuya solución es $n = 785$.

Veamos por qué.

0.°. *Resolución por la teoría de congruencias*.

Usaremos el *teorema chino de los restos*: sean $m_1, m_2, \ldots, m_k$ primos entre sí, dos a dos, sea $M = m_1 \cdot m_2 \cdot \ldots \cdot m_k$ y sean $b_1, b_2, \ldots, b_k$ enteros cualesquiera, entonces el sistema de congruencias lineales:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1}, \\ &\vdots \\ x &\equiv b_k \pmod{m_k}, \end{aligned}$$

tiene una única solución módulo M (es decir, cualquier otra solución es congruente módulo M con ésta) que es

$$x \equiv b_1 M_1 M_1' + \ldots + b_k M_k M_k' \pmod{M}, \tag{18.72}$$

siendo para todo $i = 1, 2, \ldots, k$, $M_i = M/m_i$ y M_i' el inverso único de M_i módulo m_i, esto es, la única solución de $M_i x \equiv 1 \pmod{m_i}$ (que existe al ser $\operatorname{mcd}(M_i, m_i) = 1$).

En el caso que nos ocupa, $k = 3$, $m_1 = 17$, $m_2 = 11$ y $m_3 = 6$, que son primos entre sí, dos a dos, y el teorema chino de los restos asegura que dicho sistema tiene una única solución módulo M que es (18.72) con $M = 17 \cdot 11 \cdot 6 = 1122$.

Además, como

$$\begin{aligned} M_1 &= \frac{1122}{17} = 66, \\ M_2 &= \frac{1122}{11} = 102, \\ M_3 &= \frac{1122}{6} = 187, \end{aligned}$$

y

$$\begin{aligned} 66 M_1' &\equiv 1 \pmod{17} &\to\quad M_1' &= 8, \\ 102 M_2' &\equiv 1 \pmod{11} &\to\quad M_2' &= 4, \\ 187 M_3' &\equiv 1 \pmod{6} &\to\quad M_3' &= 1, \end{aligned}$$

dicha solución es

$$n \equiv 3 \cdot 66 \cdot 8 + 4 \cdot 102 \cdot 4 + 5 \cdot 187 \cdot 1 \pmod{1122},$$

esto es,

$$n \equiv 1584 + 1632 + 935 \pmod{1122},$$

es decir,

$$n \equiv 4151 \pmod{1122}, \tag{18.73}$$

y como

$$4151 \equiv 785 \pmod{1122}, \tag{18.74}$$

(este hecho asegurará precisamente que 785 es el mínimo buscado),
entonces, por transitiva de $\equiv \pmod{1122}$ aplicada a (18.73) y (18.74),

$$n \equiv 785 \pmod{1122}.$$

Solución.— [Por la teoría de congruencias]. El mínimo número de tareas que se ha estado repartiendo siempre es $n = 785$.

1.°. *Resolución por la teoría de las ecuaciones diofánticas.*

De (18.69) y (18.70), se deduce que existen dos enteros u, v tales que

$$n = 3 + 17u, \tag{18.75}$$

$$n = 4 + 11v. \tag{18.76}$$

Restando la segunda de la primera,

$$17u - 1 = 11v,$$

esto es, $17u - 1$ es múltiplo de 11. Al representar n el número de tareas distribuidas, por las ecuaciones (18.75) y (18.76), tenemos la seguridad de que $u > 0$ y $v > 0$. Además, buscamos el menor valor para n.

Pues bien, el menor u que satisface que $11 \mid (17u - 1)$ es $u = 2$, por lo que también lo satisface cualquier u de la forma

$$u = 2 + 11t, \tag{18.77}$$

con t entero.

Sustituyendo (18.77) en (18.75), se tiene

$$n = 37 + 187t. \tag{18.78}$$

De (18.71),

$$n = 5 + 6s. \tag{18.79}$$

Restando (18.79) de (18.78),

$$6s - 187t = 32.$$

Esta ecuación es irreducible en los enteros —los números 6, 187 y 32 son (mutuamente) coprimos. Tenemos así una ecuación diofántica con dos variables; estudiémosla:

I. ¿Tiene solución entera? Sí, por el teorema 18.107 (pág. 1047 de esta edición), pues $\operatorname{mcd}(6, -187) = \operatorname{mcd}(6, 187) = 1$ y $1 | 32$.

II. Coeficientes de Bézout: $p = -31$ y $q = -1$.

III. Una solución particular es

$$s_0 = \frac{32 \cdot (-31)}{1} = -992,$$
$$t_0 = \frac{32 \cdot (-1)}{1} = -32.$$

IV. La solución general es:

$$\begin{aligned} s &= -992 + \frac{k}{1} \cdot (-187) \\ &= -992 - 187k, \qquad (18.80) \\ t &= -32 + \frac{k}{1} \cdot (-6) \\ &= -32 - 6k, \qquad (18.81) \end{aligned}$$

donde $k \in \mathbb{Z}$ (ya que $s, t \in \mathbb{Z}$).

V. Encontremos finalmente la solución particular para la cuestión en estudio. Para ello, intentemos acotar k. Al representar n el número de tareas distribuidas, por las ecuaciones (18.78) y (18.79), tenemos la seguridad de que $s > 0$ y $t > 0$.

$$\begin{aligned} 0 < s &\to 0 < 992 - 187k \\ &\to 187k < -992 \\ &\to k < \frac{-992}{187} = -5,305 \\ &\to k \in \{\dots, -8, -7, -6\}, \\ 0 < t &\to 0 < -32 - 6k \\ &\to 6k < -32 \\ &\to k < \frac{-32}{6} = -5,333 \end{aligned}$$

$$\rightarrow k \in \{\ldots, -8, -7, -6\},$$

Como (18.78) y (18.79) son monótonas crecientes para valores positivos de t y s, respectivamente, y $s = -992 - 187k$ y $t = -32 - 6k$, como funciones de k, son monótonas decrecientes para valores negativos de k, el mínimo de n se alcanza para $k = -6$, de donde, por un lado, de (18.80), $s = 130$ y, entonces, de (18.79), $n = 5 + 6 \cdot 130 = 785$, y por otro lado, de (18.87), $t = 4$ y, entonces, de (18.78), $n = 37 + 187 \cdot 4 = 785$.

Solución.— [Por la teoría de ecuaciones diofánticas]. El mínimo número de tareas que se ha estado repartiendo siempre es $n = 785$. ■

Observación 18.22.0.— Para calcular la solución al sistema de congruencias lineales, pudiésemos haber utilizado el artefacto en línea SageMath[99] y este programita en lenguaje Sage:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
crt([3, 4, 5], [17, 11, 6])
```

Observación 18.22.1.— Para calcular el máximo común divisor y los coeficientes de BÉZOUT, hubiésemos podido utilizar de nuevo el artefacto en línea SageMath y este programita en lenguaje Sage:

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
gcd(6,-187)
```

para calcular dicho máximo común divisor, y éste:

```
xgcd(6,-187)
```

para también calcular los coeficientes de BÉZOUT.

Ejemplo 609

En base diez, ¿cuáles son todos los números naturales $100\,000 \leq n \leq 999\,999$ que tienen la propiedad de ser iguales a las últimas cifras de su cuadrado (esto es, los números $n = ab..c \in [100\,000, 999\,999] \cap \mathbb{N}$ tales que $n^2 = xy..zab..c$)? (Un ejemplo entre 10 y 99 es $n = 5$ ya que $n^2 = 25$).

[EFE 14.7.2020:2a (p.h.e.c.)].

Resolución.— Los números en $[100\,000, 999\,999] \cap \mathbb{N}$ son de 6 cifras. Sean $n = ab..c$, $n^2 = xy..zab..c$ y $m = xy..z$, entonces $n^2 = 10^6 m + n$, o lo que es equivalente, $n^2 - n = 10^6 m$ o lo que

[99] *Cfr. supra* § 11 (pág. cii de esta edición).

también es equivalente,

$$n(n-1) = 10^6 m,$$

de donde $10^6 \mid n(n-1)$.

Ahora bien, como n y $n-1$ son primos entre sí y $10^6 = 2^6 \cdot 5^6$, se tiene, o bien que $\exists r, s \in \mathbb{Z}^+$ tales que $n = 2^6 r$ y $n - 1 = 5^6 s$, esto es, que

$$2^6 r - 5^6 s = 1, \tag{18.82}$$

o bien, que $\exists t, u \in \mathbb{Z}^+$ tales que $n = 5^6 t$ y $n - 1 = 2^6 u$, esto es, que

$$5^6 t - 2^6 u = 1. \tag{18.83}$$

Analicemos ambas posibilidades.

a. *La ecuación diofántica lineal* (18.82).

I. por lo establecido en el teorema 18.107 (pág. 1047 de esta edición), dicha ecuación diofántica tiene solución entera, ya que $\operatorname{mcd}(2^6, -5^6) = \operatorname{mcd}(2^6, 5^6) = 1$ y $1 \mid 1$;

II. los coeficientes de Bézout son $p = 1\,709$ y $q = 7$;

III. una solución particular es

$$r_0 = \frac{1 \cdot 1\,709}{1} = 1\,709,$$
$$s_0 = \frac{1 \cdot 7}{1} = 7;$$

IV. la solución general es

$$\begin{aligned} r &= 1\,709 + \frac{k}{1} \cdot (-5^6) \\ &= 1\,709 - 5^6 k, \end{aligned} \tag{18.84}$$

$$\begin{aligned} s &= 7 + \frac{k}{1} \cdot (-2^6) \\ &= 7 - 64k, \end{aligned} \tag{18.85}$$

siendo $k \in \mathbb{Z}$ (ya que $r, s \in \mathbb{Z}$);

V. calculemos finalmente la solución particular para la cuestión en estudio; para ello, intentemos acotar k; al representar n un número positivo, tenemos la seguridad de que $r > 0$ y $s > 0$:

$$\begin{aligned} 0 < r &\to 0 < 1\,709 - 5^6 k \\ &\to 5^6 k < 1\,709 \end{aligned}$$

$$\begin{aligned} &\to k < \frac{1\,709}{15\,625} \\ &\to k \in \{\dots, -3, -2, -1, 0\}; \\ 0 < s &\to 0 < 7 - 64k \\ &\to 64k < 7 \\ &\to k < \frac{7}{64} \\ &\to k \in \{\dots, -3, -2, -1, 0\}; \end{aligned}$$

a la vista de lo cual:

- si $k = 0$, por (18.84), $r = 1\,709$, y, por tanto, como $n = 2^6 r$, se tiene que $n = 109\,376$, y
- si $k = -1$, por (18.84), $r = 1709 + 15625 = 17334$, y, por tanto, como $n = 2^6 r$, se tendría que $n = 1\,109\,376 \notin [100\,000, 999\,999] \cap \mathbb{N}$—en realidad, como r es decreciente en k, a menor k, mayor r, por lo que el número buscado es el obtenido para $k = 0$, esto es, $n = 109\,376$—.

b. *La ecuación diofántica lineal* (18.83).

I. dicha ecuación diofántica tiene solución entera, ya que $\text{mcd}(5^6, -2^6) = \text{mcd}(5^6, 2^6) = 1$ y $1|1$;

II. los coeficientes de BÉZOUT son $p = -7$ y $q = -1709$;

III. una solución particular es

$$t_0 = \frac{1 \cdot (-7)}{1} = -7,$$
$$u_0 = \frac{1 \cdot (-1709)}{1} = -1709;$$

IV. la solución general es

$$\begin{aligned} t &= -7 + \frac{k}{1} \cdot (-2^6) \\ &= -7 - 2^6 k, \end{aligned} \tag{18.86}$$

$$\begin{aligned} u &= -1\,709 + \frac{k}{1} \cdot (-5^6) \\ &= -1\,709 - 5^6 k, \end{aligned} \tag{18.87}$$

siendo $k \in \mathbb{Z}$—ya que $t, u \in \mathbb{Z}$;

V. la solución particular para la cuestión en estudio; para ello, intentemos acotar k; al representar n un número positivo, tenemos la seguridad de que $t > 0$ y $u > 0$:

$$0 < t \to 0 < -7 - 2^6 k$$

$$\begin{aligned} &\to 2^6 k < -7 \\ &\to k < \frac{-7}{64} \\ &\to k \in \{\dots, -3, -2, -1\}; \\ 0 < u &\to 0 < -1709 - 5^6 k \\ &\to 5^6 k < -1\,709 \\ &\to k < \frac{-1\,709}{15\,625} \\ &\to k \in \{\dots, -3, -2, -1\}; \end{aligned}$$

a la vista de lo cual:

- si $k = -1$, por (18.86), $t = 57$, y, por tanto, como $n = 5^6 t$, se tiene que $n = 890\,625$, y
- si $k = -2$, por (18.86), $t = 121$, y, por tanto, como $n = 5^6 t$, se tendría que $n = 1\,890\,625 \notin [100\,000, 999\,999] \cap \mathbb{N}$—en realidad, como t es decreciente en k, a menor k, mayor t, por lo que el número buscado es el obtenido para $k = -1$, esto es, $n = 890\,625$—.

Solución.— Sólo existen dos números en $[100\,000, 999\,999] \cap \mathbb{N}$ que tienen la propiedad de ser iguales a las últimas cifras de su cuadrado, a saber, 109 376 (cuyo cuadrado es 11 963 109 376) y 890 625 (cuyo cuadrado es 793 212 890 625). ■

Observación 18.22.2.— Estos números cuyos cuadrados terminan en las mismas cifras que el número en sí se conocen como *números automorfos*[100]; en base 10 son 0, 1, 5, 6, 25, 76, 376, 625, 9 376, 90 625, 109 376, 890 625, 2 890 625, 7 109 376, 12 890 625, 87 109 376, 212 890 625, 787 109 376, 1 787 109 376, 8 212 890 625, . . . (sucesión A003226 en la OEIS[101]).

[100] *Vid. v. gr.* https://en.wikipedia.org/wiki/Automorphic_number.
[101] *Vid.* https://oeis.org/A003226.

Ejemplo 610

En Terrapaz las disputas se deciden jugando. Las personas terrapacenses se rigen por un sistema de puntos, atendiendo a su comportamiento social. Tres terrapacenses en disputa, deciden jugar varias partidas de un juego. Cada una de estas personas emplea una determinada cantidad de su total de puntos para jugar. Convienen en que la que pierda una partida, dobla los puntos de las otras dos. Al cabo de tres partidas, de las que perdió una cada persona, se dieron cuenta de que cada una tenía exactamente 8 puntos y acordaron darse por satisfechas, por lo que finalizaron el juego y zanjaron la disputa. ¿Cuántos puntos destinó cada una de las tres personas inicialmente al juego? Resolvámoslo utilizando la teoría de las ecuaciones diofánticas.

[EFE 14.7.2020:2b (p.h.e.c.)].

Resolución.— Sean X, Y, Z las tres personas terrapacenses en disputa; sean x, y, z los puntos que cada una destinó inicialmente al juego, y sean A, B y C las partidas, en ese orden. Supongamos que X pierde la partida A, Y la partida B y Z la partida C.

Por ejemplo, al perder X la partida A, ha tenido que doblar los puntos de Y y de Z, lo que a X le ha supuesto perder $y+z$ y, por tanto, quedarse con $x-(y+z)$ y a Y y Z incrementar sus cantidades en los puntos que tenían, consiguiendo un total de $y+y$ y $z+z$, respectivamente. Así se refleja en el siguiente cuadro, para ésta y las otras dos partidas: en color negro lo que tenían antes de la partida correspondiente, en verde lo que ganan y en rojo lo que pierden en dicha partida.

Tras la partida	Puntos de X	Puntos de Y	Puntos de Z
A	$x-y-z$	$y+y$	$z+z$
B	$(x-y-z)+(x-y-z)$	$2y-(x-y-z)-2z$	$2z+2z$
C	$2(x-y-z)+2(x-y-z)$	$(3y-z-x)+(3y-z-x)$	$4z-2(x-y-z)-(3y-z-x)$

El hecho es que al cabo de las tres partidas, a cada una le quedan 8 puntos. Por un lado, como el total de puntos es constante a lo largo del juego, esto nos informa de que

$$x+y+z=24$$

(en cada fila del cuadro, la suma de los puntos de X, Y y Z es $x+y+z$, el monto de puntos al inicio y siempre). Por otro, tal situación la representa el sistema de ecuaciones lineales diofánticas siguiente (una vez simplificadas las tres expresiones de la última fila del cuadro correspondientes a los puntos que les restan tras la partida C),

$$4x-4y-4z=8$$
$$-2x+6y-2z=8$$

$$-x - \ \ y + 7z = 8$$

Multiplicando la última fila por 2 y sumando las tres ecuaciones, lado a lado,

$$8z = 32,$$

de donde,

$$z = 4,$$

por lo que el sistema anterior, una vez simplificadas las ecuaciones, queda

$$\begin{aligned} x - \ \ y &= \ \ 6 \\ -x + 3y &= \ \ 8 \\ x + \ \ y &= 20 \end{aligned}$$

sumando estas tres ecuaciones se tiene la ecuación diofántica lineal

$$x + 3y = 34.$$

Resolvamos esta ecuación:

I. por lo establecido en el teorema 18.107 (pág. 1047 de esta edición), tiene solución entera, ya que $\mathrm{mcd}(1, 3) = 1$ y $1|34$;

II. los coeficientes de BÉZOUT son $p = 1$ y $q = 0$;

III. una solución particular es

$$\begin{aligned} x_0 &= \frac{34 \cdot 1}{1} = 34, \\ y_0 &= \frac{34 \cdot 0}{1} = 0; \end{aligned}$$

IV. la solución general es

$$\begin{aligned} x &= 34 + \frac{k}{1} \cdot (3) \\ &= 34 + 3k, \end{aligned} \tag{18.88}$$

$$\begin{aligned} y &= 0 + \frac{k}{1} \cdot (-1) \\ &= -k; \end{aligned} \tag{18.89}$$

V. en este punto, sustituyendo (18.88) y (18.89) en $4x - 4y - 4z = 8$, obtenemos que $k = -7$ y, por lo tanto, que $x = 13$, $y = 7$ y $z = 4$.

Solución.— La persona que perdió la primera partida destinó 13 puntos al juego, la que perdió la segunda, 7 y la que perdió la tercera, 4 puntos. ■

Observación 18.22.3.— En V, alternativamente, pudiésemos haber investigado la acotación de k; como sabemos que $x, y \in \mathbb{Z}^+$, ya que representan cantidades iniciales de puntos, se tiene que

$$\begin{aligned} 0 < x &\to 0 < 34 + 3k \\ &\to -34 < 3k \\ &\to k > \frac{-34}{3} \\ &\to k \in \{-11, -10 - 9, \dots\}, \\ 0 < y &\to 0 < -k \\ &\to k < 0 \\ &\to k \in \{\dots, -3, -2, -1\}, \end{aligned}$$

de donde $k \in \{-11, -10-9, \dots\} \cap \{\dots, -3, -2, -1\} = [-11, -1] \cap \mathbb{Z} = \{-11, -10, \dots, -1\}$, y pudiésemos calcular los valores de x, y, z según los de $k \in [-11, -1] \cap \mathbb{Z}$ y en cada caso, bien comprobando si se satisfacen para ellos las ecuaciones originales, bien calculando los puntos iniciales y verificando si el total de puntos es 24 $(= 8 \cdot 3)$; en cualquier caso, obtendríamos, igualmente, que el único valor válido es $k = -7$.

§ 18.23 Bibliografía

- Para una primera aproximación:

[205] María Dolores de PRADA VICENTE y Ricardo RODRÍGUEZ RODRÍGUEZ. *Cómo enseñar la divisibilidad*. Anaya, Madrid, Comunidad de Madrid (ES-M), España, 1982.

- Para estudiar, practicar y conocer más:

[32] Félix GARCÍA MERAYO. *Matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 2015.

[153] Francisco José GONZÁLEZ GUTIÉRREZ. *Apuntes de Matemática Discreta*. El autor, Cádiz, Andalucía (ES-AN), España, 2004.

[155] Ralph Peter GRIMALDI. *Matemáticas discreta y combinatoria*. Addison-Wesley Iberoamericana, Wilmington, New Castle, Delaware (US-DE), Estados Unidos de América, 3.ª ed., 1997.

[212] Walter MORA-FLORES. *Introducción a la teoría de números. Ejemplos y algoritmos*. Instituto Tecnológico de Costa Rica, Cartago, Cantón de Cartago, Provincia de Cartago (CR-C), República de Costa Rica, 2010. hhttps://hdl.handle.net/2238/6299. ©CC BY-NC-ND.

- Específicas sobre ecuaciones diofánticas, son:

[208] Yákov Isidórovich PERELMÁN. *Álgebra recreativa*. Mir, Moscú (RU-MOW), Distrito federal Central, Federación de Rusia, 1.ª ed., 1965. (7.ª reimpresión, 1989). (Traducido del ruso al español por C. Pérez y F. Petrov).

[209] Emiliana OLIVÁN CALZADA. Ecuaciones diofánticas. *PublicacionesDidácticas*, 26:51–62, junio 2012.

- Junto a las siguientes, que están dedicadas esencialmente a la práctica:

[150] Félix GARCÍA MERAYO, Gregorio HERNÁNDEZ PEÑALVER y Antonio NEVOT LUNA. *Problemas resueltos de matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 2018.

[197] Máximo ANZOLA GONZÁLEZ y José Ramón CARUNCHO CASTRO. *Problemas de álgebra. Tomo 2: Anillos - Polinomios - Ecuaciones.* Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1982. ©TDR.

[154] Carlos GARCÍA GÓMEZ, Josep María LÓPEZ BESORA y Dolors PUIGJANER RIBA. *Matemática discreta*. Pearson Educación, Madrid, Comunidad de Madrid (ES-M), España, 2002.

[213] Felicidad AGUADO MARTÍN, Felipe GAGO COUSO, Manuel LADRA GONZÁLEZ, Gilberto PÉREZ VEGA, Concepción VIDAL MARTÍN y Ana María VIEITES RODRÍGUEZ. *Problemas resueltos de Combinatoria. Laboratorio con SageMath*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2018.

Parte III

Razonamiento combinatorio

Íntimamente relacionada con la teoría de números, la teoría de probabilidades y la teoría de grafos, la combinatoria extiende sus ramas por los más diversos campos del conocimiento como, por ejemplo, biología, química, física, economía y lingüística, y en materias como, por ejemplo, teoría de juegos, cinética de gases, genética de poblaciones, dinámica de poblaciones y difusión de epidemias.

CAPÍTULO 19

Modelización matemática: combinatoria

C.P.: *Carissimus* (o *Clarissimus*) *puer*, *Civis publicus*, *Curavit ponendum*.

P.C.: *Pactum conventum*, *Patres conscripti*, *Pecunia constituta*, *Ponendum curavit*, *Post consulatum*, *Potestate censoria*.

(Wikipedia. *Anexo: Abreviaturas latinas — Wikipedia, La enciclopedia libre*. 2023. https://es.wikipedia.org/wiki/Anexo:Abreviaturas_latinas).

Los datos proceden de la observación o de otras fuentes; trabajamos directamente con ellos, enmarcándolos en poblaciones, muestras o unidades. Extraemos información y bosquejamos conocimiento.

Si bien en combinatoria se distinguen cinco tipos de problemas básicos, a saber, de existencia, de enumeración, de recuento, de clasificación y de optimización, en esta breve introducción nos centramos esencialmente en cuestiones de recuento estudiando cuatro modelizaciones de problemas de recuento simple: I, selección o muestreo simple; II, distribución, almacenamiento o colocación simple; III, partición simple de un conjunto, y IV, descomposición simple de un entero positivo.

Pensemos que cuando calculamos probabilidades, una de las partes más trabajosas es contar los casos favorables y los casos posibles. Para ello puede resultar útil de nuevo el conocimiento de modelos y el razonamiento por analogía. Una perspectiva estructuralista y sistémica que considere varios niveles: el nivel de las entidades (elementos), el nivel de las relaciones entre las entidades, el nivel de las relaciones entre estas relaciones y así sucesivamente, incluyendo el metanivel de todos esos niveles; elementos y relaciones articulados según determinados principios de estructura. Sin embargo, dejamos para otro momento la definición de probabilidad y el concepto de variable aleatoria como modelo de tratamiento de la incertidumbre, en definitiva, el estudio de la *modelización aleatoria*.

Por otro lado, está el uso que cada persona o artefacto hace de estas estructuras, según su manera peculiar de actuar en cada situación concreta. El examen de estos usos, sus interrelaciones y su acción sobre los principios estructurales, la posible alteración de éstos y su evolución quedan fuera del alcance de estas notas.

§ 19.0 Preliminares

§ 19.0.0 Funciones suelo, techo, redondeo y truncamiento

Definición 19.0.— Llamamos *función suelo* a la aplicación $\lfloor\,\rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$, que asigna a un número real x el mayor número entero n menor o igual que x, esto es, que está definida $\forall x \in \mathbb{R}$, $\forall n \in \mathbb{Z}$, por

$$\lfloor x \rfloor = n \leftrightarrow n \leq x < n + 1.$$

Definición 19.1.— Llamamos *función techo* a la aplicación $\lceil\,\rceil : \mathbb{R} \longrightarrow \mathbb{Z}$, que asigna a un número real x el menor número entero n mayor o igual que x, esto es, que está definida $\forall x \in \mathbb{R}$, $\forall n \in \mathbb{Z}$, por

$$\lceil x \rceil = n \leftrightarrow n - 1 < x \leq n.$$

Definición 19.2.— Llamamos *función redondeo* a la aplicación $\lfloor\,\rceil : \mathbb{R} \longrightarrow \mathbb{Z}$, que asigna a un número real x el número entero más próximo a x. La definimos a partir de las funciones suelo y techo, $\forall x \in \mathbb{R}$, por

$$\lfloor x \rceil = \begin{cases} \lceil x - 0{,}5 \rceil & \text{si} \quad x < 0 \\ \lfloor x + 0{,}5 \rfloor & \text{si} \quad x \geq 0 \end{cases}.$$

Definición 19.3.— Llamamos *función truncamiento* a la aplicación $\lceil\,\rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$, que asigna a un número real x el número entero que resulta de eliminar la parte decimal de x. La definimos a partir

de las funciones suelo y techo, $\forall x \in \mathbb{R}$, por

$$[x] = \begin{cases} \lceil x \rceil & \text{si} \quad x < 0 \\ \lfloor x \rfloor & \text{si} \quad x \geq 0 \end{cases} .$$

Pudiésemos utilizar el artefacto en línea SageMath° y el siguiente programita en lenguaje Sage, como implementación de la función truncamiento,

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/

f(x) = piecewise([ # definiendo la función truncamiento a trozos
((-oo, 0), ceil(x)), # techo de los negativos (-oo es menos infinito)
((0, oo), floor(x)), # suelo de los positivos (oo es más infinito)
([0,0],0)  # suelo de cero
])
# utilizamos show para conservar los diferentes dibujos
# utilizamos exclude=[-5..5] para excluir los puntos enteros de -5 a 5, de manera que no
    aparezcan líneas verticales
show(f(0)) #mostrando el truncamiento de cero (comprobando que lo hemos definido bien)
show(plot(floor(x),-5,5,exclude=[-5..5],color='blue')) # mostrando el dibujo en azul de la
    función suelo desde -5 a 5
show(plot(ceil(x),-5,5,exclude=[-5..5],color='red'))# mostrando el dibujo en rojo de la función
     techo desde -5 a 5
show(plot(f,-5,5,exclude=[-5..5],color='green')) # mostrando el dibujo en verde de la función
    truncamiento desde -5 a 5
show(plot(floor(x),-5,5,exclude=[-5..5],color='blue') + plot(ceil(x), -5,5,exclude=[-5..5],
    color='red') + plot(f,-5,5,exclude=[-5..5],color='green')) # dibujando las tres juntas (
    truncamiento la última para que se vea)
```

§ 19.0.1 Factoriales

Definición 19.4.— Llamamos *factorial* a la aplicación

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathbb{N} \\ n &\longmapsto n! = \begin{cases} 1 & \text{si} \quad n = 0 \\ n \cdot f(n-1) & \text{si} \quad n \geq 1 \end{cases} . \end{aligned}$$

Definición 19.5.— Llamamos *factorial de* n (o, sinónimamente, n *factorial*) a la imagen de n por la aplicación factorial, $f(n)$; notamos dicha imagen por $n!$, y es el número

$$\begin{aligned} n! &= n \cdot (n-1)! \\ &= n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1, \end{aligned}$$

° *Cfr. supra* § 11 (pág. cii de esta edición).

abreviadamente,

$$n! = \prod_{i=0}^{n-1}(n-i).$$

Observación 19.0.0.— El «equivalente» del factorial de n para la suma es el *número triangular enésimo*[1], $T_n = 1 + 2 + \cdots + n$, siendo $T_0 = 0$. Análogamente, se satisface $T_n = T_{n-1} + n$, para $n \geq 1$.

Definición 19.6.— Llamamos *número factorial descendente de n de orden k* al número

$$n^{\underline{k}} = n(n-1)(n-2)\ldots(n-k+1),$$

abreviadamente,

$$n^{\underline{k}} = \prod_{i=0}^{k-1}(n-i).$$

Otra notación frecuente para el número factorial descendente de n de orden k es $(n)_k$.

Teorema 19.0

Se satisface:

0. $n^{\underline{n}} = n!$;
1. $n^{\underline{n-k}} \cdot k! = n!$;
2. $n^{\underline{k}} \cdot (n-k)! = n!$.

Actividad 19.0

Demostremos este teorema a partir de las definiciones anteriores.

Teorema 19.1 (Recurrencias)

Se satisface:

0. $n^{\underline{k+1}} = n^{\underline{k}} \cdot (n-k)$;
1. $(n+1)^{\underline{k+1}} = n^{\underline{k}} \cdot (n+1)$.

Actividad 19.1

Demostremos este teorema a partir de las definiciones anteriores.

Definición 19.7.— Llamamos *número factorial ascendente de n de orden k* al número

$$n^{\overline{k}} = n(n+1)(n+2)\ldots(n+k-1),$$

[1] *Vid. infra* observación 20.3.7 (pág. 1310 de esta edición).

abreviadamente,

$$n^{\overline{k}} = \prod_{i=0}^{k-1}(n+i).$$

Otra notación frecuente para el número factorial ascendente de n de orden k es $n^{(k)}$.

Teorema 19.2 (Interrelaciones entre el factorial descendente y el ascendente)
Se satisface:
0. $n^{\overline{k}} = (n+k-1)^{\underline{k}}$;
1. $n^{\underline{k}} = (n-k+1)^{\overline{k}}$.

Actividad 19.2

Demostremos este teorema a partir de las definiciones anteriores.

Actividad 19.3

¿Son 1, 2, 145 y 40585 los únicos números decimales iguales a la suma de los factoriales de sus dígitos?*

* *Vid. v. gr.* https://en.wikipedia.org/wiki/Factorion.

§ 19.0.2 Factoriales y números primos

Definición 19.8.— Llamamos *primo factorial* a un número primo que es igual a un factorial menos uno o a un factorial más uno.[2]

La sucesión de primos factoriales (2, 3, 5, 7, 23, 719, 5039, 39916801, 479001599, 87178291199, . . .) está catalogada en la OEIS como la sucesión A088054[3].

A fecha de hoy se desconoce si existe un número infinito de primos factoriales.

Definición 19.9.— Llamamos *primorial del número primo* p_n al número

$$p_n\# = p_1 \cdot p_2 \cdot \ldots \cdot p_n,$$

esto es, al producto de los n primeros números primos.[4]

La sucesión de primoriales $p_n\#$ (1, 2, 6, 30, 210, 2310, 30030, 510510, 9699690, . . .) está catalogada en la OEIS como la sucesión A002110[5].

[2] *Vid. v. gr.* https://en.wikipedia.org/wiki/Factorial_prime.
[3] *Vid.* https://oeis.org/A088054.
[4] *Vid. v. gr.* https://en.wikipedia.org/wiki/Primorial#Definition_for_prime_numbers.
[5] *Vid.* https://oeis.org/A002110.

Definición 19.10.— Llamamos *primo primorial*[6] a un número primo de la forma $p_n\# \pm 1$.

A fecha de hoy se desconoce si existe un número infinito de primos primoriales y tampoco si el número de números de la forma $p_n\# \pm 1$ es infinito.

Definición 19.11.— Llamamos *primorial del número entero positivo* n al número

$$n\# = \prod_{\substack{p \leq n \\ p,\ \text{primo}}} p,$$

esto es, al producto de los números primos menores o iguales que n.[7]

La sucesión de primoriales $n\#$ (1, 1, 2, 6, 6, 30, 30, 210, 210, 210, 210, 2310, 2310, 30030, ...) está catalogada en la OEIS como la sucesión A034386[8].

§ 19.0.3 Coeficiente binomial

Definición 19.12.— Llamamos *coeficiente binomial* (o, sinónimamente, *número combinatorio*), al número

$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!},$$

siendo $n, k \in \mathbb{N}$ y $k \leq n$.

Observación 19.0.1.— En particular,

0. $\forall n \in \mathbb{N}$, $\binom{n}{0} = 1$;
1. si $n < k$ o $k < 0$, $\binom{n}{k} = 0$.

[6] *Vid. v. gr.* https://en.wikipedia.org/wiki/Primorial_prime.
[7] *Vid. v. gr.* https://en.wikipedia.org/wiki/Primorial#Definition_for_natural_numbers.
[8] *Vid.* https://oeis.org/A034386.

Teorema 19.3 (Algunas propiedades satisfechas por los coeficientes binomiales, I)

Se satisface, $\forall h, k, k_0, \ldots, k_p, m, n, n_0, \ldots, n_p, p \in \mathbb{N}$:

0. $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ si $k \leq n$;
1. $\binom{n}{0} = \binom{n}{n} = 1$;
2. $\binom{n}{1} = \binom{n}{n-1} = n$;
3. $\binom{n}{k} = \binom{n}{n-k}$ si $k \leq n$; (complementación)
4. $\binom{n}{k} = \dfrac{n}{k}\binom{n-1}{k-1}$ si $1 \leq k \leq n$;
5. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ si $1 \leq k \leq n$; (identidad de Pascal)
6. $\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$ si $k \leq m \leq n$;
7. $\binom{n+1}{k+1} = \sum_{i=k}^{n} \binom{i}{k}$ si $k \leq n$;
8. $\sum_{k=0}^{h} \binom{m}{k}\binom{n}{h-k} = \binom{m+n}{h}$; (identidad de Vandermonde, 1772; Zhu Shijie, 1303)
9. $\binom{n_0 + \cdots + n_p}{m} = \sum_{k_0+\cdots+k_p=m} \binom{n_0}{k_0} \cdots \binom{n_p}{k_p}$. (id. de Vandermonde generalizada)

Se conoce como *triángulo aritmético* (o, sinónimamente, *triángulo de* Pascal o *triángulo de* Tartaglia[9]), la siguiente disposición de los coeficientes binomiales:

[9] El teorema del binomio y el triángulo fueron descubiertos varios siglos antes en la matemática china por Yang Hui, Zhu Shijie y Jia Xian, en la matemática india por los matemáticos védicos y jain, con el nombre de *meru-prastara*, y en la matemática árabe por los discípulos de Al-Karaji.

$$\begin{array}{c}\binom{0}{0}\\ 1\end{array}$$

$$\begin{array}{cc}\binom{1}{0} & \binom{1}{1}\\ 1 & 1\end{array}$$

$$\begin{array}{ccc}\binom{2}{0} & \binom{2}{1} & \binom{2}{2}\\ 1 & 2 & 1\end{array}$$

$$\begin{array}{cccc}\binom{3}{0} & \binom{3}{1} & \binom{3}{2} & \binom{3}{3}\\ 1 & 3 & 3 & 1\end{array}$$

$$\begin{array}{ccccc}\binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4}\\ 1 & 4 & 6 & 4 & 1\end{array}$$

$$\begin{array}{cccccc}\binom{5}{0} & \binom{5}{1} & \binom{5}{2} & \binom{5}{3} & \binom{5}{4} & \binom{5}{5}\\ 1 & 5 & 10 & 10 & 5 & 1\end{array}$$

$$\begin{array}{ccccccc}\binom{6}{0} & \binom{6}{1} & \binom{6}{2} & \binom{6}{3} & \binom{6}{4} & \binom{6}{5} & \binom{6}{6}\\ 1 & 6 & 15 & 20 & 15 & 6 & 1\end{array}$$

$$\begin{array}{cccccccc}\binom{7}{0} & \binom{7}{1} & \binom{7}{2} & \binom{7}{3} & \binom{7}{4} & \binom{7}{5} & \binom{7}{6} & \binom{7}{7}\\ 1 & 7 & 21 & 35 & 35 & 21 & 7 & 1\end{array}$$

$$\begin{array}{ccccccccc}\binom{8}{0} & \binom{8}{1} & \binom{8}{2} & \binom{8}{3} & \binom{8}{4} & \binom{8}{5} & \binom{8}{6} & \binom{8}{7} & \binom{8}{8}\\ 1 & 8 & 28 & 56 & 70 & 56 & 28 & 8 & 1\end{array}$$

$$\begin{array}{cccccccccc}\binom{9}{0} & \binom{9}{1} & \binom{9}{2} & \binom{9}{3} & \binom{9}{4} & \binom{9}{5} & \binom{9}{6} & \binom{9}{7} & \binom{9}{8} & \binom{9}{9}\\ 1 & 9 & 36 & 84 & 126 & 126 & 84 & 36 & 9 & 1\end{array}$$

$$\begin{array}{ccccccccccc}\binom{10}{0} & \binom{10}{1} & \binom{10}{2} & \binom{10}{3} & \binom{10}{4} & \binom{10}{5} & \binom{10}{6} & \binom{10}{7} & \binom{10}{8} & \binom{10}{9} & \binom{10}{10}\\ 1 & 10 & 45 & 120 & 210 & 252 & 210 & 120 & 45 & 10 & 1\end{array}$$

$$\begin{array}{cccccccccccccc}\binom{n}{0} & \binom{n}{1} & \binom{n}{2} & \binom{n}{3} & \binom{n}{4} & \binom{n}{5} & \cdots & \binom{n}{n-5} & \binom{n}{n-4} & \binom{n}{n-3} & \binom{n}{n-2} & \binom{n}{n-1} & \binom{n}{n}\\ \frac{n!}{0!n!} & \frac{n!}{1!(n-1)!} & \frac{n!}{2!(n-2)!} & \frac{n!}{3!(n-3)!} & \frac{n!}{4!(n-4)!} & \frac{n!}{5!(n-5)!} & & \frac{n!}{(n-5)!1!} & \frac{n!}{(n-4)!2!} & \frac{n!}{(n-3)!3!} & \frac{n!}{(n-2)!4!} & \frac{n!}{(n-1)!5!} & \frac{n!}{n!0!}\\ \vdots & & & & & \vdots & & \vdots & & & & & \ddots\end{array}$$

Observación 19.0.2.— Se satisface:

0. Cada fila comienza y termina por uno;
1. cada uno de los otros números se obtiene sumando los dos números de encima de él, por ejemplo, $1+9=10$, $28=21+7$, $120=84+36$ (la identidad de Pascal —*cfr. supra* teorema 19.3.5 (pág. 1130)— expresa esta propiedad).

Teorema 19.4 (Teorema binomial —NEWTON—)

Se satisface, $\forall x, y \in \mathbb{R}, \forall n \in \mathbb{N}$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Observación 19.0.3.— La fórmula (19.4) es conocida como *fórmula binomial*. Se satisface:

0. $(x+y)^n = \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} x^0 y^n;$

1. $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k};$

2. $(x+1)^n = (1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$

Teorema 19.5 (Corolario: algunas potencias destacadas de binomios)
Se satisface, $\forall x, y \in \mathbb{R}$:

0. $(x \pm y)^2 = x^2 \pm 2xy + y^2;$
1. $(x \pm y)^3 = x^3 \pm 3x^2y + 3xy^2 \pm y^3;$
2. $(x \pm y)^4 = x^4 \pm 4x^3y + 6x^2y^2 \pm 4xy^3 + y^4;$
3. $(x \pm y)^5 = x^5 \pm 5x^4y + 10x^3y^2 \pm 10x^2y^3 + 5xy^4 \pm y^5;$
4. $(x \pm y)^6 = x^6 \pm 6x^5y + 15x^4y^2 \pm 20x^3y^3 + 15x^2y^4 \pm 6xy^5 + y^6.$

Observación 19.0.4.— Fijémonos en cómo los coeficientes (salvo signos) están en el triángulo de Pascal en la línea correspondiente a la potencia del binomio; por ejemplo, los coeficientes de $(x \pm y)^5$, salvo signo, son 1, 5, 10, 10, 5, 1, que se sitúan en el nivel 5 del triángulo (el vértice superior es el nivel 0).

Teorema 19.6 (Algunas factorizaciones destacadas)
Se satisface, $\forall x, y \in \mathbb{R}$:

0. $x^2 - y^2 = (x-y)(x+y);$
1. $x^3 \pm y^3 = (x \pm y)(x^2 \pm xy + y^2);$
2. $x^5 \pm y^5 = (x \pm y)(x^4 \pm x^3y + x^2y^2 \pm xy^3 + y^4).$

Observación 19.0.5.— Existen muchísimas interrelaciones, a modo de ejemplo la *identidad de* LEGENDRE: $(x+y)^2 - (x-y)^2 = 4xy$.

Teorema 19.7 (Algunas propiedades satisfechas por los coeficientes binomiales, II)
Se satisface:

10. $\forall n \in \mathbb{Z}^+$,
$$\binom{n+k-1}{k} = \frac{n^{\overline{k}}}{k!};$$

11. Simetría: $\forall n \in \mathbb{Z}^+$,
$$\binom{n+k-1}{k} = \binom{n+k-1}{n-1};$$

Teorema 19.8 (Algunas propiedades satisfechas por los coeficientes binomiales, III)

Se satisface:

12. Cardinal del conjunto potencia: $\forall n \in \mathbb{N}$,

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n;$$

13. $\forall n \in \mathbb{N}$,

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = 2^{n-1};$$

14. $\forall n \in \mathbb{N}$,

$$\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1};$$

15. $\forall n \in \mathbb{N}, n \geq 2$,

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots = n2^{n-1};$$

Teorema 19.9 (Algunas propiedades satisfechas por los coeficientes binomiales, IV)

Se satisface:

16. $\forall n \in \mathbb{N}$,

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n} = 0;$$

17. $\forall n \in \mathbb{N}$,

$$\binom{n}{0} - \binom{n}{1} + 2 \cdot \binom{n}{2} - \cdots + (-1)^{n+1} \cdot n \binom{n}{n} = 0.$$

Teorema 19.10 (Algunas propiedades satisfechas por los coeficientes binomiales, V)

Se satisface:

18. Fórmula del «palo de hockey»: $\forall n, k \in \mathbb{N}$,

$$\binom{n}{n} + \binom{n+1}{n} + \cdots + \binom{n+k}{n} = \binom{n+k+1}{n+1};$$

19. $\forall n \in \mathbb{N}$,

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n};$$

20. $\forall m, n \in \mathbb{N}$,

$$\binom{m}{0} + \binom{1+m}{1} + \binom{2+m}{2} + \cdots + \binom{n+m}{n} = \binom{n+m+1}{n};$$

Teorema 19.11 (Algunas propiedades satisfechas por los coeficientes binomiales, VI)
Se satisface:

21. $\forall n \in \mathbb{N}, \forall k \in \mathbb{N} \setminus \{0, 1\}$,

$$\binom{n+2}{k} = \binom{n}{k} + 2 \cdot \binom{n}{k-1} + \binom{n}{k-2};$$

22. Teorema de la estrella de David (GOULD, 1972): $\forall n, k \in \mathbb{N} \setminus \{0, 1\}$,

$$\operatorname{mcd}\left\{\binom{n-1}{k-1}, \binom{n}{k+1}, \binom{n+1}{k}\right\} = \operatorname{mcd}\left\{\binom{n-1}{k}, \binom{n}{k-1}, \binom{n+1}{k+1}\right\}.$$

§ 19.0.4 Coeficiente multinomial

Definición 19.13.— Sean $n, p, k_0, k_1, \ldots, k_p \in \mathbb{N}$; llamamos *coeficiente multinomial* al número

$$\binom{n}{k_0, k_1, \ldots, k_p} = \frac{n!}{k_0! \cdot k_1! \cdots k_p!}.$$

Teorema 19.12 (Teorema multinomial —LEIBNIZ—)
Dados $n, p \in \mathbb{N}$, se satisface

$$(x_0 + x_1 + \cdots + x_p)^n = \sum_{k_0+k_1+\cdots+k_p=n} \binom{n}{k_0, k_1, \ldots, k_p} x_0^{k_0} x_1^{k_1} \cdots x_p^{k_p},$$

donde $k_0, \ldots, k_p \in \mathbb{N}$ y existen tantos sumandos como posibles sumas $k_0 + k_1 + \cdots + k_p$ iguales a n.

Ejemplo 611

Demostremos que $\forall x, y, z \in \mathbb{R}$, $(x+y+z)^2 = x^2 + y^2 + z^2 + 2xy + 2xz + 2yz$.

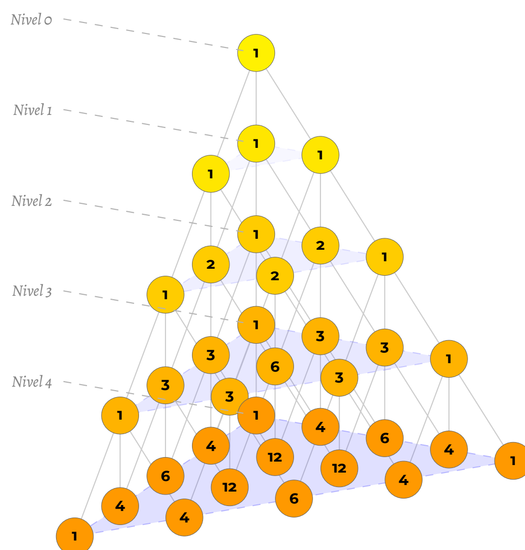
Resolución.— En efecto,

$$\begin{aligned}(x+y+z)^2 &= \binom{2}{2,0,0}x^2 + \binom{2}{0,2,0}y^2 + \binom{2}{0,0,2}z^2 + \binom{2}{1,1,0}xy + \binom{2}{1,0,1}xz + \binom{2}{0,1,1}yz \\ &= x^2 + y^2 + z^2 + 2xy + 2xz + 2yz.\end{aligned}$$

■

Observación 19.0.6.— El teorema del binomio de NEWTON es el caso particular del teorema multinomial de LEIBNIZ para $p = 1$.

A modo de ejemplo, la siguiente disposición de los *coeficientes trinomiales*, conocida como *pirámide (o tetraedro) de* Pascal:



Teorema 19.13 (Corolario: algunas potencias destacadas de trinomios)
Se satisface, $\forall x, y, z \in \mathbb{R}$:

0. $(x+y+z)^2 = x^2+y^2+z^2+2xy+2xz+2yz$;
1. $(x+y+z)^3 = x^3+y^3+z^3+3x^2y+3x^2z+3xy^2+3y^2z+3xz^2+3yz^2+6xyz$;
2. $(x+y+z)^4 = x^4+y^4+z^4+4x^3y+4x^3z+4xy^3+4y^3z+4xz^3+4yz^3+6x^2y^2+6x^2z^2+6y^2z^2+12x^2yz+12xy^2z+12xyz^2$;
3. $(x+y+z)^5 = x^5+y^5+z^5+5x^4y+5x^4z+5xy^4+5y^4z+5xz^4+5yz^4+10x^3y^2+10x^3z^2+10x^2y^3+10y^3z^2+10x^2z^3+10y^2z^3+20x^3yz+20xy^3z+20xyz^3+30x^2y^2z+30x^2yz^2+30xy^2z^2$;
4. $(x+y+z)^6 = x^6+y^6+z^6+6x^5y+6x^5z+6xy^5+6y^5z+6xz^5+6yz^5+15x^4y^2+15x^4z^2+15x^2y^4+15y^4z^2+15x^2z^4+15y^2z^4+20x^3y^3+20x^3z^3+20y^3z^3+30x^4yz+30xy^4z+30xyz^4+60x^3y^2z+60x^3yz^2+60x^2y^3z+60xy^3z^2+60x^2yz^3+60xy^2z^3+90x^2y^2z^2$.

Teorema 19.14 (Generalización de la identidad de Pascal)
Sean $k_0, k_1, \ldots, k_p, n, p \in \mathbb{Z}^+$, tales que $k_0+k_1+\cdots+k_p = n$; entonces

$$\begin{aligned}\binom{n}{k_0, k_1, k_2, \ldots, k_p} = \binom{n-1}{k_0-1, k_1, k_2, \ldots, k_p} &+ \binom{n-1}{k_0, k_1-1, k_2, \ldots, k_p}\\ &+ \binom{n-1}{k_0, k_1, k_2-1, \ldots, k_p}\\ &\ \vdots\\ &+ \binom{n-1}{k_0, k_1, k_2, \ldots, k_p-1}.\end{aligned}$$

§ 19.1 Principios fundamentales de recuento

§ 19.1.0 Principio de la adición

Teorema 19.15
Si un suceso S_0 puede ocurrir de m formas distintas y un suceso S_1 de n formas distintas, y no pueden ocurrir ambos sucesos a la vez, entonces, el suceso unión $S_0 \cup S_1$, puede ocurrir de $m + n$ formas distintas.

Esto se extiende a un número finito de sucesos, incompatibles dos a dos. Notemos por $\#S$ el número de formas en que sucede un suceso S.

Teorema 19.16
Dados $S_0, S_1, \ldots, S_k$, sucesos incompatibles dos a dos —o incompatibles consecutivamente dos a dos—, se satisface que el número de formas en que sucede el suceso unión $S_0 \cup S_1 \cup \ldots \cup S_k$, es la suma de los números de formas en que suceden los sucesos, esto es,

$$\#\left(\bigcup_{i=0}^{k} S_i\right) = \sum_{i=0}^{k} \#S_i.$$

También es posible enunciarlo en términos de conjuntos, ya extendido a un número finito de conjuntos.

Teorema 19.17
Dados $X_0, X_1, \ldots, X_k$, conjuntos finitos disjuntos dos a dos, se satisface que el cardinal del conjunto unión $X_0 \cup X_1 \cup \ldots \cup X_k$, es la suma de los cardinales de los conjuntos, esto es,

$$\left|\bigcup_{i=0}^{k} X_i\right| = \sum_{i=0}^{k} |X_i|.$$

Ejemplo 612

Utilicemos razonadamente el principio de la adición para calcular el número total de saludos que tienen lugar en una reunión a la que asisten n personas en la que todas se saludan entre sí una, y sólo una, vez. Para ello: 0.°, formalicemos la situación según el principio de la adición; 1.°, razonemos de cuántas formas sucede cada uno de los sucesos intervinientes, y 2.°, finalmente, apliquemos el principio de la adición.

[EFE 22.6.2022:7], [SEL 9:1c]. *Cfr. v. gr.* Franco, Espinel y Almeida [214]: ejercicio 3.20 (pág. 43).

Resolución.— Veamos.

0.°, *Formalización del principio de la adición.*

Para poder aplicar el principio de la adición debemos definir sucesos incompatibles —o incompatibles consecutivamente— dos a dos. Para ello, sin pérdida de generalidad, numeremos las personas (comenzamos en 1 por claridad de la exposición), dispongámoslas en una fila y pensemos que se saludan en orden: la primera saluda al resto de $n-1$ personas de la fila, tras lo que se retira de la misma; la segunda —que ahora ocupa la primera posición en la fila— saluda al resto de $n-2$ personas de la fila, tras lo que se retira de la misma; la tercera —que ahora ocupa la primera posición en la fila— saluda al resto de $n-3$ personas de la fila, tras lo que se retira de la misma, y así sucesivamente, la persona $n-2$ saluda a dos personas (a las personas $n-1$ y a la n) y, finalmente, la persona $n-1$ saluda a una persona (a la persona n).

De este modo, pudiésemos hablar de los sucesos

$$\begin{aligned} S_1 &\fallingdotseq \text{la primera persona saluda,} \\ S_2 &\fallingdotseq \text{la segunda persona saluda,} \\ &\vdots \\ S_{n-1} &\fallingdotseq \text{la persona } (n-1)\text{-ésima saluda.} \end{aligned}$$

que son incompatibles dos a dos consecutivamente, puesto que cada persona, al retirarse de la fila, saluda a cada una de las demás una única vez.

1.°, *De las formas de suceder los sucesos.*

El suceso S_1 sucede de $n-1$ formas distintas; el suceso S_2, de $n-2$ formas distintas; en general, para $1 \leq i \leq n-1$, el suceso $S_i \fallingdotseq$ la persona iésima saluda, sucede de $n-i$ formas distintas.

2.°, *Aplicación del principio de la adición.*

Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_1 \cup S_2 \cup \ldots \cup S_{n-1}$. Como hemos dicho ya, son sucesos incompatibles dos a dos consecutivamente —ya que la

persona i ya ha sido saludada por la persona $i-1$ y, por tanto, no va a volver a saludarla—, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

$$\begin{aligned}\#(S_1 \cup S_2 \cup \ldots \cup S_{n-1}) &= \#S_1 + \#S_2 + \ldots + \#S_{n-1} \\ &= (n-1)+(n-2)+\ldots+2+1. \end{aligned} \quad \blacksquare$$

Observación 19.1.0.— La suma $1+2+\cdots+(n-2)+(n-1)$ es la de los $n-1$ primeros términos de una progresión aritmética de diferencia 1, esto es,

$$(1+(n-1))\cdot\frac{n-1}{2} = \frac{n\cdot(n-1)}{2}.$$

Demostración.— Recordemos la anécdota de Gauss, siendo un niño, en clase (seguramente, para $n=50$):

$$\begin{array}{ccccccccccc} s_n & = & 1 & + & 2 & + & \ldots & + & (n-1) & + & n \\ s_n & = & n & + & (n-1) & + & \ldots & + & 2 & + & 1, \end{array}$$

de donde, sumando, obtenemos

$$2s_n \;=\; (n+1) \;+\; (n+1) \;+\; \ldots \;+\; (n+1) \;+\; (n+1),$$

y de aquí,

$$2s_n = n(n+1),$$

por lo que

$$s_n = \frac{n(n+1)}{2}. \blacksquare$$

Observación 19.1.1.— En la formulación del principio con conjuntos disjuntos dos a dos, éstos son $S_i = \{x : x \text{ es saludada por } i\}$ y sus cardinales, $|S_i| = n-i$.

Observación 19.1.2.— *Cfr. infra* ejemplo 749 (pág. 1366 de esta edición).

§ 19.1.1 Principio de la multiplicación

Teorema 19.18

Si un suceso S puede ocurrir en dos fases sucesivas e independientes, S_0 y S_1, y existen m formas distintas de realizar la fase S_0 y n formas distintas de realizar la fase S_1, independientemente de cómo se haya realizado la fase S_0, entonces existen $m\cdot n$ formas diferentes en las que puede ocurrir el suceso S.

Observación 19.1.3.— «Independientemente de cómo se haya realizado la fase S_0», no de qué se haya realizado en la fase S_0.

Esto se extiende a un número finito de fases sucesivas, independientes consecutivamente.

Teorema 19.19
Si un suceso S puede ocurrir en un número finito de fases sucesivas e independientes consecutivamente $S_0, S_1, \ldots, S_k$ (la realización de S_{i+1} es independiente de cómo se haya realizado S_i), se satisface que el número de formas en que puede ocurrir el suceso S es el producto de los números de formas en que se realizan las fases, esto es

$$\#S = \prod_{i=0}^{k} \#S_i.$$

También es posible enunciarlo en términos de conjuntos, ya extendido a un número finito de conjuntos.

Teorema 19.20
Dados $X_0, X_1, \ldots, X_k$, conjuntos finitos, se satisface

$$\left| \bigtimes_{i=0}^{k} X_i \right| = \prod_{i=0}^{k} |X_i| .$$

Ejemplo 613

Calculemos el número total de números capicúas de seis cifras en base seis (un número es capicúa si se lee igual de izquierda a derecha que de derecha a izquierda). Para ello: 0.º, formalicemos la situación según el principio de la multiplicación, el suceso y sus fases; 1.º, razonemos de cuántas formas puede realizarse cada una de las fases, y 2.º, finalmente, apliquemos el principio de la multiplicación.

[EFE 7.7.2017:5a] (de siete cifras, en base diez), [SEL 9:1b]. *Cfr. v. gr.* Franco, Espinel y Almeida [214]: ejercicios 3.6-3.7 (pág. 48).

Resolución.— Veamos.

0.º, *Formalización del principio de la multiplicación: del suceso y sus fases.*

Un número senario[10] capicúa de seis cifras tiene la forma $abccba$, con $a, b, c \in \{0, 1, 2, 3, 4, 5\}$ y $a \neq 0$. Observemos que para hallar las cifras basta considerar abc.

Intuitivamente, vemos que existen cinco posibilidades para a, seis para b y otras seis para c.

[10] El *sistema de numeración senario* (o, sinónimamente, *heximal* o *seximal*) tiene seis como su base (*vid. v. gr.* https://en.wikipedia.org/wiki/Senary).

Formalmente, para poder aplicar el principio de la multiplicación debemos definir un suceso descompuesto en fases sucesivas e independientes consecutivamente.

Sea el suceso

$$S \risingdotseq \text{la «construcción» del número senario } abc,$$

que ocurre en tres fases sucesivas e independientes:

$$\begin{aligned} S_0 &\risingdotseq \text{la «construcción» de la cifra senaria } a, \\ S_1 &\risingdotseq \text{la «construcción» de la cifra senaria } b, \\ S_2 &\risingdotseq \text{la «construcción» de la cifra senaria } c. \end{aligned}$$

que son sucesivas e independientes consecutivamente.

1.°, *De las formas de realizar las fases*.

- Fase S_0: existen cinco formas distintas de realizarla, ya que a puede ser 1, 2, 3, 4 o 5.
- Fase S_1: existen seis formas distintas de realizarla, ya que a puede ser 0, 1, 2, 3, 4 o 5.
- Fase S_2: existen seis formas distintas de realizarla, ya que a puede ser 0, 1, 2, 3, 4 o 5.

2.°, *Aplicación del principio de la multiplicación*.

Nuestro interés es averiguar el número de formas en que sucede el suceso S. Como hemos dicho ya, S ocurre en tres fases sucesivas e independientes, así que es admisible aplicar el principio de la multiplicación. Notando por $\#X$ el número de formas en que ocurre un suceso X y también el número de formas en que se realiza una fase X, existen

$$\begin{aligned} \#S &= \#S_0 \cdot \#S_1 \cdot \#S_2 \\ &= 5 \cdot 6 \cdot 6 \\ &= 180 \end{aligned}$$

formas de que ocurra el suceso S. ■

Observación 19.1.4.— En la formulación del principio con conjuntos disjuntos dos a dos, éstos son $S_0 = \{x : x \in \mathbb{N} \wedge 1 \leq x < 6\}$, $S_1 = S_0 \cup \{0\}$, $S_2 = S_1$ y sus cardinales, $|S_0| = 5$, $|S_1| = 6$ y $|S_2| = 6$.

Observación 19.1.5.— Ya que hemos mencionado los números (senarios) capicúas, pudiésemos ver esta demostración, sencilla e instructiva, ofrecida por Marta Macho Stadler[11], de que *no existen números primos capicúas, excepto el* 11, *con un número par de cifras*: https://ztfnews.wordpress.com/2014/06/06/no-hay-numeros-primos-palindromicos-con-un-numero-par-de-cifras/.

[11] *Vid. v. gr.* https://es.wikipedia.org/wiki/Marta_Macho_Stadler.

[Cubit 126].

Por cierto, *se conjetura que el número de primos capicúas*[12] *es infinito*.

Ejemplo 614

¿Cuántos números naturales menores que 1000 tienen todas sus cifras distintas? Para ello: 0.º, formalicemos la situación según el principio de la adición; 1.º, razonemos de cuántas formas sucede cada uno de los sucesos intervinientes, y 2.º, finalmente, apliquemos el principio de la adición.

[Cubit 137].

Resolución.— Los naturales menores que 1000 tienen una, dos o tres cifras. Vamos a aplicar el principio de la adición y a la hora de calcular algunos números de formas en que suceden los sucesos, el de multiplicación.

0.°, *Formalización del principio de la adición: de los sucesos*.

Distinguimos los sucesos:

$$S_0 \coloneqq \text{ser un número natural de una cifra,}$$
$$S_1 \coloneqq \text{ser un número natural de dos cifras con sus cifras distintas,}$$
$$S_2 \coloneqq \text{ser un número natural de tres cifras con todas sus cifras distintas,}$$

que son incompatibles dos a dos (por ejemplo, S_1 y S_2 son sucesos incompatibles porque no existe un número natural con dos y tres cifras a la vez).

El suceso $S \coloneqq$ ser un número natural menor que 1000 con todas sus cifras distintas es $S = S_0 \cup S_1 \cup S_2$.

1.°, *De las formas en que suceden los sucesos*.

A. De una cifra, hay 10 números naturales, del 0 al 9.

B. Para dos cifras, vamos a aplicar el principio de la multiplicación.

0.°, *Formalización del principio de la multiplicación: del suceso y sus fases*.

Un número decimal de dos cifras tiene la forma ab, con $a, b \in \{x : x \in \mathbb{N} \wedge 0 \leq x < 10\}$ y $a \neq 0$.

Para poder aplicar el principio de la multiplicación debemos definir un suceso descompuesto en fases sucesivas e independientes consecutivamente.

[12] *Vid. v. gr.* https://en.wikipedia.org/wiki/Palindromic_prime.

Sea el suceso

$$S \leftrightharpoons \text{la «construcción» del número decimal de dos cifras } ab,$$

que ocurre en dos fases sucesivas e independientes consecutivamente (la realización de S_1 es independiente de cómo se haya realizado S_0 —no de qué se haya hecho, sino de cómo—):

$$S_0 \leftrightharpoons \text{la «construcción» de la cifra decimal } a,$$
$$S_1 \leftrightharpoons \text{la «construcción» de la cifra decimal } b.$$

1.°, *De la forma de realizar las fases.*

- Fase S_0: existen nueve formas distintas de realizarla, ya que a, la cifra de las decenas, tiene nueve posibles valores (del 1 al 9).
- Fase S_1: existen nueve formas distintas de realizarla, ya que b, la cifra de las unidades, tiene nueve posibles valores, del 0 al 9 excluyendo la cifra de las decenas (estamos contando números con cifras distintas).

2.°, *Aplicación del principio de la multiplicación.*

El principio de multiplicación establece que el número de formas en que sucede el suceso S es igual al producto de los números de formas en que se realizan sus fases, esto es, existen formas de que suceda S. En efecto,

$$\begin{aligned} \#S &= \#S_0 \cdot \#S_1 \\ &= 9 \cdot 9 \\ &= 81. \end{aligned}$$

C. Para tres cifras, el razonamiento es análogo al anterior hecho para dos cifras. Resumido, es: hay 9 posibilidades para la cifra de las centenas (del 1 al 9), otras 9 para la de las decenas (del 0 al 9 excluyendo la de las centenas) y otras 8 para la cifra de las unidades (del 0 al 9 excluyendo la de las centenas y la de las decenas), así, por el principio de la multiplicación hay $9 \cdot 9 \cdot 8 = 648$.

2.°, *Aplicación del principio de la adición.*

El principio de la adición establece que el número de formas en que sucede el suceso $S = S_0 \cup S_1 \cup S_2$ es igual a la suma de los números de formas en que suceden los sucesos S_0, S_1 y S_2, esto es,

$$\#S = \#S_0 + \#S_1 + \#S_2$$

$$= 10 + 81 + 648$$
$$= 739.$$ ■

Actividad 19.4

Demostremos que el número de divisores positivos de un número entero positivo es el que establece el teorema 18.20 (pág. 963 de esta edición).

[SEL 9:1a]. *Cfr.* Franco, Espinel y Almeida [214]: ejercicio 3.10 (pág. 49).

§ 19.1.2 Principio del complementario

Teorema 19.21

Dado un conjunto X e $Y \subseteq X$, se satisface

$$|Y| = |X| - |X \setminus Y|,$$

siendo $X \setminus Y$ el complementario de Y en X.

Ejemplo 615

Sirva el ejemplo 657 (pág. 1189 de esta edición) como tal.

§ 19.1.3 Principio de la división

Teorema 19.22 (Principio de la división)

Un suceso S que ocurre de n formas, en realidad ocurre de n/d formas distintas si cualquier forma r, a su vez, ocurre de d de las n formas (formas distintas no pueden ocurrir de la misma forma, esto es, notando D_x el conjunto de formas en que ocurre la forma x, entonces si dos formas r y s son distintas, $D_r \cap D_s = \emptyset$).

También es posible enunciarlo en términos de conjuntos.

Teorema 19.23

Sea X un conjunto finito unión de n subconjuntos disjuntos dos a dos, cada uno de cardinal d, entonces

$$n = \frac{|X|}{d}.$$

Y en términos de funciones.

Teorema 19.24
Si $f : X \longrightarrow C$ transforma el conjunto finito X sobre C y si $\forall c \in C$ los conjuntos $f^{-1}(c) = \{x \in X : f(x) = c\}$ son disjuntos dos a dos y tienen el mismo número de elementos, digamos d, entonces

$$|C| = \frac{|X|}{d}.$$

Ejemplo 616

En una frase aparecen treinta palabras distintas con diferentes atributos (sean éstos semánticos, morfológicos, fonológicos, pragmáticos, en definitiva, un predicado relativo a la palabra —por ejemplo, tener el mismo número de vocales—), cada atributo es compartido por seis palabras y ninguna palabra tiene más de un atributo de los considerados. Entonces debe haber cinco atributos. ¿Por qué?

Resolución.—

- En la formulación del principio de la división en términos de sucesos, S es el suceso ser una palabra de la frase, suceso que sucede de treinta formas (en treinta palabras), si bien como a cada palabra le acompaña su atributo y la caracteriza en este contexto, tenemos que en realidad sucede de $30/6 = 5$ formas distintas (las cinco representantes de las cinco clases de palabras según sus atributos).
- En la formulación del principio de la división en términos de conjuntos, X es el conjunto de treinta palabras, unión de los subconjuntos disjuntos de palabras que comparten cada atributo, $A_i = \{$ palabras que comparten el atributo $i\}$, y $d = 6$, por lo que el número de atributos es $n = 5$ (tantos como subconjuntos disjuntos).
- En la formulación en términos de funciones, X es el conjunto de palabras, C el conjunto de atributos, y f la función que asigna a cada palabra su atributo. ■

§ 19.1.4 Principio de los cajones (DIRICHLET)

Teorema 19.25 (Principio restringido de los cajones de DIRICHLET)
Si distribuimos k objetos en n cajones y $n < k$, entonces hay al menos un cajón que contiene al menos dos objetos.

Ejemplo 617

Demostremos que dados tres números enteros, la suma de dos de ellos es par.

[SEL 9:3].

Resolución.— Observemos que para elaborar un esquema de resolución basado en los requisitos para aplicar el principio restringido de los cajones de Dirichlet, tenemos que formalizar la situación determinando cuáles y cuántos son los objetos y cuáles y cuántos son los cajones, y que el número de cajones sea menor que el de objetos.

Consideramos tres objetos ($k = 3$), los tres números enteros, y dos cajones ($n = 2$), el cajón de los números pares y el cajón de los números impares; entonces, como $n = 2 < 3 = k$, del principio restringido de los cajones de Dirichlet se sigue que hay un cajón que contiene al menos dos objetos, esto es, de los tres números enteros, o bien dos son pares o bien dos son impares, y en ambos casos, la suma es par (si ambos son pares, $2m + 2n = 2(m + n)$; si ambos son impares, $2m + 1 + 2n + 1 = 2(m + n) + 2 = 2(m + n + 1)$). ■

Teorema 19.26 (Principio generalizado de los cajones de Dirichlet)
Si se distribuyen k objetos en n cajones y $n < k$, entonces:
0.º, al menos un cajón contiene como mínimo $\lceil k/n \rceil$ objetos, y
1.º, al menos un cajón contiene como máximo $\lfloor k/n \rfloor$ objetos.

Ejemplo 618

En una presentación de proyectos se puntúa con las puntuaciones enteras no negativas 0, 1, 2, 3. Nos preguntamos: 0.º, ¿cuál es el mínimo número de proyectos para que al menos siete reciban la misma puntuación?, y 1.º, ¿cuál es el mínimo número de proyectos para que como máximo siete reciban la misma puntuación?

[Cubit 138].

Resolución.—

0.º, Cuatro cajones ($n = 4$), los cajones de las puntuaciones 0, 1, 2 y 3. Según el principio generalizado de los cajones de Dirichlet, tenemos que encontrar el menor k tal que $\lceil k/4 \rceil \geq 7$, donde $\lceil \rceil$ es la función techo. (Los objetos son los proyectos y su número k es lo que debemos averiguar). Observemos que $\lceil 24/4 \rceil = \lceil 6 \rceil = 6$ y $\lceil 25/4 \rceil = \lceil 6{,}25 \rceil = 7$. En palabras: si hubiese $4 \cdot 6 = 24$ proyectos, podrían recibir cada seis de ellos la misma puntuación, así que si hay $4 \cdot 6 + 1 = 25$ proyectos seguro que al menos siete reciben la misma puntuación.

1.°, Según el principio generalizado de los cajones de Dirichlet, tenemos que encontrar el menor k tal que $\lfloor k/4 \rfloor \leq 7$, donde $\lfloor\,\rfloor$ es la función suelo. La respuesta es $k = 1$, sólo un proyecto. (Por si no nos convenciese esta respuesta, neguémosla: ¿hay acaso más de siete proyectos que reciben la máxima puntuación?). ■

Ejemplo 619

Del conjunto de números naturales $\{1, 2, \ldots, 33\}$ elegimos siete números distintos. Demostremos que al menos dos de estos siete son tales que su diferencia es como mucho cinco.

[Cubit 139].

Resolución.— Sean $n_0, n_1, \ldots, n_6 \in \{1, 2, \ldots, 33\}$ los números elegidos. Supongamos, sin pérdida de generalidad, que $n_0 < n_1 < \cdots < n_6$. Debemos razonar sobre la diferencia entre dos números. Consideremos la suma de las diferencias entre consecutivos, $(n_1 - n_0) + (n_2 - n_1) + \cdots + (n_6 - n_5)$. Esta suma es igual a $n_6 - n_0$ y menor o igual que $33 - 1 = 32$.

¿Por qué hacemos esto? Veamos.

Consideremos $n = 6$ cajones, los 6 sumandos.

$n_1 - n_0$ | $n_2 - n_1$ | $n_3 - n_2$ | $n_4 - n_3$ | $n_5 - n_4$ | $n_6 - n_5$

Los objetos son $k = 32$ unos (objetos indistinguibles). Consideremos ahora que un valor numérico es una suma de unos e imaginemos por un momento que los números $n_0, n_1, \ldots, n_6$ fuesen 1, 2, 4, 7, 11, 16, 22, entonces la suma de las diferencias entre consecutivos sería

$$1 + 2 + 3 + 4 + 5 + 6,$$

un total de $22 - 1 = 21$ objetos, suma que es posible reescribir como

$$1 + (1 + 1) + (1 + 1 + 1) + (1 + 1 + 1 + 1) + (1 + 1 + 1 + 1 + 1) + (1 + 1 + 1 + 1 + 1 + 1),$$

es decir, en el primer cajón habría un objeto (representado por un uno), en el segundo habría dos objetos (dos unos), y así sucesivamente hasta el último cajón en el que habría seis objetos (seis unos).

Como $6 < 32$ (esto es, $n < k$), entonces del principio generalizado de los cajones de Dirichlet se sigue que existe al menos un cajón que contiene como máximo $\lfloor 32/6 \rfloor = 5$ objetos, esto es, existe como mínimo un sumando menor o igual que 5, en otras palabras, al menos dos de los siete números elegidos son tales que su diferencia es como mucho 5. ■

Observación 19.1.6.— Esto es un ejemplo de codificación.

Actividad 19.5

Apliquemos el principio de los cajones (generalizado o no) de Dirichlet para demostrar que dados cinco puntos interiores de un triángulo equilátero de lado dos unidades, al menos dos de esos puntos distan, como máximo, una unidad.

[SEL 9:2a]. *Cfr.* FRANCO, ESPINEL y ALMEIDA [214], ejemplo 3.15 (pág. 39).

Observación 19.1.7.— A propósito del principio de los cajones. Ejemplos de su aplicación:

- en *Una de mates*[13]: Una de mates: el principio del palomar[14];
- en *Matemoción*[15]:
  - El principio del palomar, una potente herramienta matemática (parte 1)[16];
  - El principio del palomar, una potente herramienta matemática (parte 2)[17].

§ 19.1.5 Principio de inclusión-exclusión

Teorema 19.27 (Principio de inclusión-exclusión)

Sean $X_0, X_1, \ldots, X_n$, conjuntos finitos, e $I_m = \{0, 1, 2, \ldots, m\}$; se satisface:

0. $|X_0 \cup X_1| = |X_0| + |X_1| - |X_0 \cap X_1|$;
1. $$|X_0 \cup X_1 \cup X_2| = |X_0| + |X_1| + |X_2| - |X_0 \cap X_1| - |X_0 \cap X_2| - |X_1 \cap X_2| + |X_0 \cap X_1 \cap X_2| = \sum_{i=0}^{2} |X_i| - \sum_{i<j} |X_i \cap X_j| + |X_0 \cap X_1 \cap X_2| \quad (i, j \in I_2);$$
2. $$\left|\bigcup_{i=0}^{3} X_i\right| = \sum_{i=0}^{3} |X_i| - \sum_{i<j} |X_i \cap X_j| + \sum_{i<j<k} |X_i \cap X_j \cap X_k| - \left|\bigcap_{i=0}^{3} X_i\right| \quad (i, j, k \in I_3);$$
3. $$\left|\bigcup_{i=0}^{n} X_i\right| = \sum_{i=0}^{n} |X_i| - \sum_{i<j} |X_i \cap X_j| + \sum_{i<j<k} |X_i \cap X_j \cap X_k| - \cdots + (-1)^n \left|\bigcap_{i=0}^{n} X_i\right| \quad (i, j, k \in I_n).$$

Ejemplo 620

Vid. ejemplo 307 (pág. 564 de esta edición) y el apág. 2 del ejemplo 373 (pág. 710 de esta edición).

Observación 19.1.8.— El principio de inclusión-exclusión aparece en algunos textos con una notación más compacta. Sean $X_0, X_1, \ldots, X_n$, conjuntos finitos, $I_n = \{0, 1, 2, \ldots, n\}$ y 2^{I_n} el conjunto potencia de I_n; se satisface

[13] *Vid*. https://culturacientifica.com/categoria/una-de-mates/.
[14] *Vid*. https://culturacientifica.com/2015/10/06/una-de-mates-el-principio-del-palomar/.
[15] *Vid*. https://culturacientifica.com/categoria/matemocion/.
[16] *Vid*. https://culturacientifica.com/2015/02/11/el-principio-del-palomar-una-potente-herramienta-matematica-parte-1/.
[17] *Vid*. https://culturacientifica.com/2015/02/25/el-principio-del-palomar-una-potente-herramienta-matematica-parte-2/.

$$\left|\bigcup_{i=0}^{n} X_i\right| = \sum_{J\in 2^{I_n}\setminus\emptyset} (-1)^{|J|+1}\left|\bigcap_{j\in J} X_j\right|.$$

§ 19.1.6 Desorden

Definición 19.14.— Llamamos *desorden* a una permutación en la que ninguno de sus elementos aparece en la posición original.

Ejemplo 621 (El problema del guardarropa)

Un grupo de doce personas visita un museo. Todas llevan abrigo de lana. Al entrar, los dejan en el guardarropa. Al salir, la persona encargada pone sobre el mostrador los doce abrigos. Completamente distraídas por una conversación muy interesante, cada persona del grupo coge uno al azar. Empleemos un razonamiento combinatorio para determinar de cuántas formas puede ocurrir que ninguna haya cogido su abrigo.

Cfr. Matoušek y Nešetřil [124]: 2.8 La dama del guardarropa (págs. 99ss.).
Para saber más: E738 – *Solutio quaestionis curiosae ex doctrina combinationum*, http://eulerarchive.maa.org/.

Resolución.— Se trata de encontrar el número de desórdenes de 12 objetos. En vez de para 12, vamos a calcularlo para n. Sea $\{1, 2, \ldots, n\}$. Siendo P el conjunto de todas las permutaciones y P_k el conjunto de todos los desórdenes que fijan k elementos, entonces, el conjunto de todos los desórdenes es

$$D = P - \left(\bigcup_{i=1}^{n} P_i\right).$$

Veamos:

- ¿Cuántas permutaciones fijan un número concreto? Pues las permutaciones del resto, $n-1$, o sea, $(n-1)!$ y como hay n números, son $(n-1)!\cdot n$ las permutaciones que fijan un número cualquiera (subyace el principio de la multiplicación).
- ¿Cuántas permutaciones fijan dos números concretos? Pues las permutaciones del resto, $n-2$, o sea, $(n-2)!$ y como hay $C(n,2)$ formas de elegir dos números distintos entre n, son $(n-2)!\cdot C(n,2)$ las permutaciones que fijan dos números cualesquiera (subyace el principio de la multiplicación).

Observemos que en el caso $n = 2$, esto es, $\{1, 2\}$, al restar las que fijan el 1, se resta una vez las que fijan el 1 y el 2 y al restar las que fijan el 2 se resta otra vez las que fijan el 1 y el 2, por lo que hay que sumarlos una vez. Si seguimos este análisis, el número de permutaciones que no conserva ningún

número en su lugar (desórdenes) es:

$$\begin{aligned}|D| &= |P| - \left|\left(\bigcup_{i=1}^{n} P_i\right)\right| \\ &= \binom{n}{0} n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \cdots + (-1)^{n+1}\binom{n}{n} 0!\end{aligned}$$

Así, para el caso de ser $n = 12$, existen

$$\binom{12}{0} 12! - \binom{12}{1}(12-1)! + \binom{12}{2}(12-2)! - \cdots + (-1)^{12+1}\binom{12}{12} 0! = 176\,214\,841$$

desórdenes.

Solución.— De 176 214 841 formas. ■

Actividad 19.6

En el ejemplo inmediatamente anterior hemos aplicado el principio de la multiplicación, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Veamos ahora un teorema y su demostración que reforzará lo pensado en el ejemplo anterior a la par que introduciremos la definición de subfactorial.

Teorema 19.28

El número de desórdenes de un conjunto de n elementos es

$$n!\left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^n}{n!}\right),$$

abreviadamente,

$$n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Este número se conoce como *subfactorial de* n y se nota $!n$.

Demostración.— Sea un conjunto de n elementos $C = \{c_0, c_1, \ldots, c_{n-1}\}$. Aplicaremos el *principio del complementario*. Sea B el conjunto de las permutaciones de C; sabemos que $|B| = n!$. Sea A el conjunto de los desórdenes de C, por lo que $B \setminus A$ es el conjunto de las permutaciones de C que dejan fijo algún elemento, esto es, el conjunto de las que dejan fijo c_0 unión el conjunto de las que dejan fijo c_1 y así sucesivamente hasta su unión con el conjunto de las que dejan fijo c_{n-1}. Formalicemos esto último: si llamamos S_k al conjunto de permutaciones que dejan fijo el kaésimo elemento, c_k, con $0 \leq k < n$, entonces $B \setminus A = S_0 \cup \cdots \cup S_{n-1}$.

Por el *principio de inclusión-exclusión*, siendo $I_{n-1} = \{0, 1, 2, \ldots, n-1\}$,

$$\begin{aligned}|B \setminus A| &= |S_0 \cup \cdots \cup S_{n-1}| \\ &= \sum_i |S_i| - \sum_{i<j} \left|S_i \cap S_j\right| + \sum_{i<j<k} \left|S_i \cap S_j \cap S_k\right| - \cdots + (-1)^{n-1} \left|\bigcap_{i=0}^{n-1} X_i\right| \quad (i, j, k \in I_{n-1}).\end{aligned}$$

Observemos que la primera suma es el total de permutaciones que dejan fijo un elemento, la segunda el total de permutaciones que dejan fijos dos elementos, la tercera el total de permutaciones que dejan fijos tres elementos, etc.

Formalicémoslo utilizando el *principio de la multiplicación*. Sea $S = \{S_0, S_1, \ldots, S_{n-1}\}$. Entonces:

- elegimos un subconjunto R de S, de cardinal h (esta elección es la fase 0), existiendo $C(n, h)$ subconjuntos de S de cardinal h (éste es el número de formas en que es posible realizar la fase 0), y
- observamos que la intersección de h conjuntos S_i distintos, fija h elementos (esta acción de la intersección es la fase 1), existiendo $(n-h)!$ permutaciones que hacen tal cosa (éste es el número de formas en que es posible realizar la fase 1).

Del principio de la multiplicación se sigue que el número de permutaciones correspondiente a todos los posibles subconjuntos de S de cardinal h es $C(n, h) \cdot (n-h)!$.

Por lo tanto, del principio de inclusión-exclusión se sigue

$$\begin{aligned}|B \setminus A| &= \binom{n}{1}(n-1)! - \binom{n}{2}(n-2)! + \binom{n}{3}(n-3)! - \cdots + (-1)^{n-1}\binom{n}{n}0! \\ &= \sum_{i=1}^{n} (-1)^{i-1} \binom{n}{i} (n-i)! \\ &= n! \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i!} \\ &= n! \sum_{i=1}^{n} \frac{(-1)^{i+1}}{i!} \\ &= n! \left(\frac{(-1)^2}{1!} + \frac{(-1)^3}{2!} + \cdots + \frac{(-1)^{n+1}}{n!} \right),\end{aligned}$$

y como un desorden es una permutación que no deja fijo ninguno de los n elementos, entonces, por el principio del complementario,

$$\begin{aligned}|A| &= |B| - |B \setminus A| \\ &= n! - |S_0 \cup \cdots \cup S_{n-1}| \\ &= n! \left(1 - \left(\frac{(-1)^2}{1!} + \frac{(-1)^3}{2!} + \cdots + \frac{(-1)^{n+1}}{n!} \right)\right)\end{aligned}$$

$$= n!\left(\frac{(-1)^0}{0!} - (-1)\left(\frac{(-1)^1}{1!} + \frac{(-1)^2}{2!} + \cdots + \frac{(-1)^n}{n!}\right)\right)$$
$$= n!\sum_{i=0}^{n}\frac{(-1)^i}{i!}$$
$$= !n. \qquad \blacksquare$$

Observación 19.1.9.—

0. $!n = \lfloor n!/e \rceil \quad (1 \leq n)$.
1. El subfactorial $!n$ está catalogado como la sucesión A000166 en la OEIS[18].

Observación 19.1.10.— Aunque en estas notas sólo estudiamos ecuaciones en diferencias lineales con coeficientes constantes, no está de más saber que el subfactorial satisface las ecuaciones

$$!n = (n-1)(!(n-2) + !(n-1)),$$
$$!n = n \cdot !(n-1) + (-1)^n,$$

ambas demostradas por Euler.

[SEL 13:6].

Ejemplo 622

En un examen tipo test de 16 cuestiones de opción múltiple, con 4 opciones cada una, en el que 4 cuestiones son del bloque I, 6 del bloque II y 6 del bloque III:

0. ¿De cuántas formas pueden reordenarse por bloques las cuestiones de manera que ninguna esté en su posición original?
1. En una cuestión, ¿de cuántas formas pueden reordenarse las opciones de manera que ninguna esté en su posición original?
2. ¿Cuántas variantes del examen existen de manera que ninguna cuestión esté en su posición original dentro de su bloque y tampoco ninguna opción de ninguna cuestión esté en su posición original?

Resolución.—

0. Por el teorema 19.28 (pág. 1149 de esta edición):
   - bloque I: subfactorial de 4, esto es, $!4 = 9$ desórdenes;
   - bloque II: $!6 = 265$ desórdenes;

[18] *Vid*. https://oeis.org/A000166.

- bloque III: $!6 = 265$ desórdenes;

por lo tanto, por el principio de la multiplicación, existen $9 \cdot 265 \cdot 265 = 632\,025$ formas.

1. Por dicho teorema, existen $!4 = 9$ formas.
2. Por el principio de la multiplicación, existen $632\,025 \cdot 9 = 5\,688\,225$ variantes. ■

Ejemplo 623

¿Cuántos términos del desarrollo de un determinante de orden n contienen uno o más elementos de la diagonal de la matriz correspondiente?

Resolución.— De nuevo aplicaremos el principio del complementario.

El determinante de la matriz $A = \begin{pmatrix} a_{1,1} \dots a_{1,n} \\ \vdots \quad \vdots \\ a_{n,1} \dots a_{n,n} \end{pmatrix}$, calculado por la fórmula de LEIBNIZ, es $\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$ (comenzamos en 1 por claridad de la exposición).

Cada sumando se corresponde con una permutación, por lo que el número de sumandos es el número de permutaciones en el grupo S_n, esto es, $n!$.

Contener un elemento de la diagonal es que en la permutación σ suceda que $\sigma(i) = i$ para un i, es decir que σ tenga un punto fijo.

No contener ningún elemento de la diagonal es el suceso complementario al anterior, que la permutación correspondiente no fije ningún punto. En definitiva, contar los términos que no contienen ningún elemento de la diagonal es contar las permutaciones que no fijan ningún punto, en otras palabras, contar los desórdenes.

Sea $C = \{1, 2, \dots, n\}$ el conjunto de índices para las filas y las columnas. Sea B el conjunto de las permutaciones de C; sabemos que $|B| = n!$. Sea A el conjunto de las permutaciones de C que dejan fijo algún elemento, por lo que $B \setminus A$ es el conjunto de los desórdenes de C.

Del teorema 19.28 (pág. 1149 de esta edición) sabemos que $|B \setminus A| = !n$.

Por el principio del complementario:

$$\begin{aligned} |A| &= |B| - |B \setminus A| \\ &= n! - !n \\ &= n! - n! \sum_{i=0}^{n} \frac{(-1)^i}{i!} \\ &= n! \left(1 - \left(\frac{(-1)^0}{0!} + \frac{(-1)^1}{1!} + \frac{(-1)^2}{2!} + \dots + \frac{(-1)^n}{n!}\right)\right) \end{aligned}$$

$$= n!\left(1 - 1 + 1 - \frac{1}{2!} + \cdots + \frac{(-1)^n}{n!}\right)$$
$$= n!\left(1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} + \cdots + \frac{(-1)^n}{n!}\right).$$

Solución.— En un determinante de orden n, el número de términos del desarrollo que contienen uno o más elementos de la diagonal de la matriz es

$$n!\left(1 - \frac{1}{2!} + \frac{1}{3!} - \frac{1}{4!} + \cdots + \frac{(-1)^n}{n!}\right).$$ ■

§ 19.2 Primeras operaciones combinatorias

Estudiadas en la educación secundaria, anticipadas en estas notas (*cfr. supra* § 6 [pág. lxxxiv de esta edición]) y algunas ya utilizadas en los ejemplos anteriores, es la hora de definir y estudiar en mayor profundidad estas primeras *operaciones combinatorias*, a saber, variaciones, permutaciones y combinaciones, ordinarias y con repetición, y su número.

§ 19.2.0 Variación

Definición 19.15.— Una *variación* de k elementos de un conjunto no vacío X es cualquier aplicación inyectiva de $\{0, 1, \dots, k-1\}$ en X.

Ejemplo 624

Proporcionemos dos ejemplos de variación de tres elementos del conjunto $X = \{a, b, c, d, e\}$.

[Cubit 132].

Resolución.— Dado el conjunto $X = \{a, b, c, d, e\}$, un ejemplo de variación de tres elementos de X es la aplicación $0 \longmapsto a, 1 \longmapsto c, 2 \longmapsto d$, que abreviamos con la tupla $\langle a, c, d\rangle$; esta variación es una aplicación distinta de, por ejemplo, $0 \longmapsto d, 1 \longmapsto a, 2 \longmapsto c$, abreviadamente, $\langle d, a, c\rangle$, que constituye el otro ejemplo pedido. ■

Observación 19.2.0.— El concepto de variación se corresponde con lo que en cursos anteriores nos comentaron de ser la variación el caso en que «importaba el orden de disposición de los elementos, ninguno de éstos se repetía y no intervenían necesariamente todos».

Teorema 19.29

Una *variación* de k elementos de un conjunto no vacío X es cualquier aplicación inyectiva de un conjunto de k elementos en X.

Demostración.— Esto es así porque por tener igual cardinal existe una aplicación biyectiva entre $\{0, 1, \ldots, k-1\}$ y cualquier conjunto de k elementos, digamos Y, y ser, por tanto, la composición resultante una aplicación inyectiva de $\{0, 1, \ldots, k-1\}$ en X. ∎

Teorema 19.30

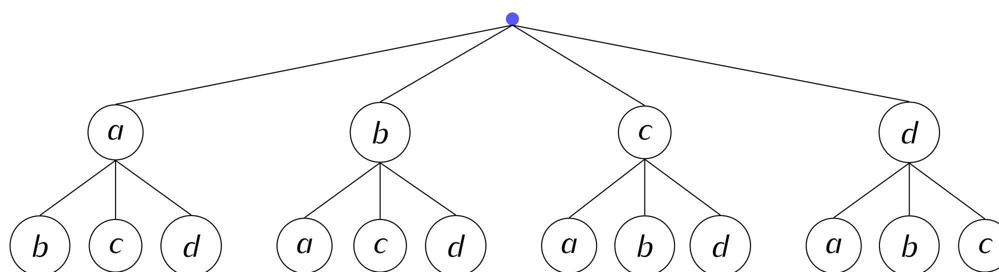
Si X tiene n elementos, siendo $n \geq k$, el *número de variaciones* de k elementos de X es $n^{\underline{k}}$, esto es, $n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-k+1)$. $V(n, k)$ (o, sinónimamente, $V_{n,k}$, V_k^n, ${}_nV_k$, ${}^nV_k$ o V_n^k) designa dicho número. Si $n < k$, no existen variaciones.

Ejemplo 625

Siendo el alfabeto $\Sigma = \{a, b, c, d\}$, ¿cuántas palabras de Σ^2 existen en las que no se repiten letras?

Resolución.— Una palabra corresponde a una aplicación inyectiva del conjunto de posiciones $\{0, 1\}$ en el conjunto Σ, ya que ninguna letra puede ser la imagen de más de una posición al no poder repetirse ninguna letra en la palabra. Por lo tanto, cada palabra es una variación de 2 elementos de Σ, de donde el número de palabras es el número de variaciones, esto es, es posible formar $VR(4, 2) = 4^{\underline{2}} = 4 \cdot 3 = 12$ palabras de longitud 2 en las que no se repite ninguna letra.

Pudiésemos ilustrar esto con un árbol:



Como vemos, cada rama (esto es, cada camino desde la raíz) es una palabra de longitud dos en la que no se repite ninguna letra. ∎

Actividad 19.7

Resolvamos el ejemplo anterior por el principio de la multiplicación.

Ejemplo 626 (PRen1)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir tres tareas distinguibles entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si ninguno de éstos puede recibir más de una?

[EFE 29.1.2025:10] (tipo test).

Resolución.— Cada reparto corresponde a una aplicación inyectiva del conjunto de tareas $\{t, t', t''\}$ en el conjunto no vacío C de computadores auxiliares $\{c_1, c_2, \ldots, c_7\}$ (inyectiva porque ningún computador auxiliar puede recibir más de una tarea), así, diremos que cada reparto es una variación de tres elementos de C; el número de posibles repartos es el número de variaciones, por lo tanto, existen $V(7,3) = 7^{\underline{3}} = 7 \cdot 6 \cdot 5 = 210$ formas posibles de repartir las tareas. ■

Observación 19.2.1.— Notemos la similitud con una resolución posible del ejemplo anterior por el principio de la multiplicación ($7 \cdot 6 \cdot 5$ han sido las formas).

Observación 19.2.2.— Notemos también que todo ha consistido en seleccionar ordenadamente (el orden de los computadores importa para distinguir dos muestras) los tres computadores auxiliares que han recibido una tarea cada uno; selección sin reemplazamiento, ya que un computador auxiliar puede ser seleccionado sólo una vez (no puede recibir más de una tarea) (*cfr. infra*. cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—).

Observación 19.2.3.— Es posible interpretar un reparto desde diferentes puntos de vista conceptuales; por ejemplo, entre otros, como una selección de computadores (observación anterior), o como una distribución o asignación de las tareas a los computadores (estas interpretaciones corresponden a las modelizaciones I y II que estudiaremos más adelante).

§ 19.2.1 Variación con repetición

Definición 19.16.— Una *variación con repetición* de k elementos de un conjunto no vacío X es cualquier aplicación de $\{0, 1, \ldots, k-1\}$ en X.

Ejemplo 627

Proporcionemos dos ejemplos de variación con repetición de 4 elementos del conjunto $X = \{a, b, c, d, e\}$.

Resolución.— Dado el conjunto $X = \{a, b, c, d, e\}$, un ejemplo de variación con repetición de 4 elementos de X es la definida por $0 \longmapsto a$, $1 \longmapsto c$, $2 \longmapsto d$, $3 \longmapsto c$, que abreviamos con la tupla

$\langle a, c, d, c\rangle$; esta variación con repetición es una aplicación distinta de, por ejemplo, la definida por $0 \longmapsto d, 1 \longmapsto a, 2 \longmapsto c, 3 \longmapsto c$, abreviadamente, $\langle d, a, c, c\rangle$, que constituye el otro ejemplo pedido. ■

Observación 19.2.4.— El concepto de variación con repetición se corresponde con lo que en cursos anteriores nos comentaron de ser la variación con repetición el caso en que «importaba el orden de disposición de los elementos, algunos de éstos se repetían y no intervenían necesariamente todos».

Teorema 19.31

Una *variación con repetición* de k elementos de un conjunto no vacío X es cualquier aplicación de un conjunto de k elementos en X.

Demostración.— Esto es así porque por tener igual cardinal existe una aplicación biyectiva entre $\{0, 1, \ldots, k-1\}$ y cualquier conjunto de k elementos, digamos Y, y ser, por tanto, la composición resultante una aplicación de $\{0, 1, \ldots, k-1\}$ en X. ■

Teorema 19.32

Si X tiene n elementos, el *número de variaciones con repetición* de k elementos de X es n^k. $VR(n, k)$ (o, sinónimamente, $VR_{n,k}$, VR_k^n, ${}_nVR_k$, ${}^nVR_k$ o VR_n^k) designa dicho número.

Ejemplo 628

Siendo el alfabeto $\Sigma = \{a, b, c, d, e, f\}$, ¿cuántas palabras tienen longitud 21?

Resolución.— Una palabra corresponde a una aplicación cualquiera del conjunto de posiciones $\{0, 1, 2, \ldots, 20\}$ en el conjunto Σ, sin ninguna condición, ya que una letra puede ser la imagen de varias posiciones (por ejemplo, en la palabra $aababcabcdabcdeabcdef$ la única letra que es imagen de una sola posición es la f). Por lo tanto, cada palabra es una variación con repetición de 21 elementos de Σ, de donde el número de palabras es el número de variaciones con repetición, esto es, es posible formar $VR(6, 21) = 6^{21}$ palabras de longitud 21 con las letras de Σ, en otras palabras, $|\Sigma^{21}| = 6^{21}$. ■

Actividad 19.8

Siendo el alfabeto $\Sigma = \{a, b, c, d, e, f\}$, ¿cuántas palabras de Σ^3 no tienen letras repetidas?

Ejemplo 629 (PRen2)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir tres tareas distinguibles entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si cualquiera de éstos puede recibir cualquier número de tareas?

Resolución.— Cada reparto corresponde a una aplicación cualquiera del conjunto de tareas $\{t, t', t''\}$ en el conjunto no vacío A de computadores auxiliares $\{c_1, c_2, \ldots, c_7\}$ (sin ninguna condición, pues dice que cualquier computador auxiliar puede recibir cualquier número de tareas), así, diremos que cada reparto es una variación con repetición de tres elementos de A; el número de posibles repartos es el número de variaciones con repetición, por lo tanto, existen $VR(7, 3) = 7^3 = 7{\cdot}7{\cdot}7 = 343$ formas posibles de repartir las tareas. ■

Observación 19.2.5.— Notemos la similitud con una resolución posible del ejemplo anterior por el principio de la multiplicación ($7 \cdot 7 \cdot 7$ han sido las formas).

Observación 19.2.6.— Notemos también que todo ha consistido en seleccionar ordenadamente los tres computadores auxiliares que han recibido una tarea cada uno; selección con reemplazamiento, ya que un computador auxiliar puede ser seleccionado más de una vez (puede recibir más de una tarea) (*cfr. infra*. cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—).

Ejemplo 630

¿Cuántas palabras ternarias de longitud 15 contienen al menos un 0, al menos un 1 y al menos un 2?

Resolución.— El número de palabras ternarias de longitud 15 es $VR(3, 15) = 3^{15} = 14\,348\,907$ (pensemos por qué).

Sea S el conjunto de todas las palabras ternarias de longitud 15, entonces $|S| = 3^{15}$.

Sean:

$$S_0 = \{x \in S : x \text{ no tiene ningún cero}\};$$
$$S_1 = \{x \in S : x \text{ no tiene ningún uno}\};$$
$$S_2 = \{x \in S : x \text{ no tiene ningún dos}\}.$$

Sea $B = \{x \in S : x \text{ tiene al menos un cero, al menos un uno y al menos un dos}\}$, por lo que $B^\complement = \{x \in S : x \text{ no tiene ningún cero o no tiene ningún uno o no tiene ningún dos}\}$.

Nos interesa calcular $|B|$ y por el *principio del complementario* sabemos que $|B| = |S| - |B^{\complement}|$, es decir, $|B| = |S| - |S_0 \cup S_1 \cup S_2|$.

Sabemos (pensemos por qué):

$$\begin{aligned} |S_0| = |S_1| = |S_2| = VR(2,15) = 2^{15} = 32\,768; \\ |S_0 \cap S_1| = |S_0 \cap S_2| = |S_1 \cap S_2| = 1; \\ |S_0 \cap S_1 \cap S_2| = 0. \end{aligned}$$

(Pensemos, por ejemplo, en que $|S_0 \cap S_1| = \{22\ldots 2\}$, $|S_0 \cap S_2| = \{11\ldots 1\}$ y $|S_1 \cap S_2| = \{00\ldots 0\}$. ¿Y el último?, ¿cuántas palabras no tienen ni ceros, ni unos, ni doses? Pues ninguna, es cuestión de leer las definiciones de los conjuntos S_i y preguntarnos sobre sus cardinales...).

Aplicando el *principio de inclusión-exclusión*,

$$\begin{aligned} |S_0 \cup S_1 \cup S_2| &= |S_0| + |S_1| + |S_2| - |S_0 \cap S_1| - |S_0 \cap S_2| - |S_1 \cap S_2| + |S_0 \cap S_1 \cap S_2| \\ &= 2^{15} + 2^{15} + 2^{15} - 1 - 1 - 1 + 0 \\ &= 3 \cdot (2^{15} - 1) \\ &= 98\,301, \end{aligned}$$

por tanto,

$$\begin{aligned} |B| &= |S| - |S_0 \cup S_1 \cup S_2| \\ &= 3^{15} - 3 \cdot (2^{15} - 1) \\ &= 14\,348\,907 - 98\,301 \\ &= 14\,250\,606. \end{aligned}$$

Solución.— Existen catorce millones doscientos cincuenta mil seiscientas seis palabras ternarias de longitud 15 que contienen al menos un 0, al menos un 1 y al menos un 2. ■

Actividad 19.9

Terminemos la demostración del teorema 1.3 (pág. 74 de esta edición).

§ 19.2.2 Permutación

Definición 19.17.— Una *permutación* de los elementos de un conjunto finito X es cualquier aplicación biyectiva de X en X.

Teorema 19.33
Una *permutación* de los elementos de un conjunto finito X de n elementos es cualquier aplicación biyectiva de un conjunto de n elementos en X.

Demostración.— Esto es así porque por tener igual cardinal existe una aplicación biyectiva entre X y cualquier conjunto de n elementos, digamos Y, y ser, por tanto, la composición resultante una aplicación biyectiva de X en X. ■

Ejemplo 631

Proporcionemos dos ejemplos de permutación del conjunto $X = \{a, b, c, d, e\}$.

Resolución.— Dado el conjunto $X = \{a, b, c, d, e\}$, un ejemplo de permutación de X es $0 \longmapsto a, 1 \longmapsto c, 2 \longmapsto d, 3 \longmapsto e, 4 \longmapsto b$, que abreviamos con la tupla $\langle a, c, d, e, b\rangle$; esta permutación es una aplicación distinta de, por ejemplo, la definida por $0 \longmapsto d, 1 \longmapsto a, 2 \longmapsto c, 3 \longmapsto b, 4 \longmapsto e$, abreviadamente, $\langle d, a, c, b, e\rangle$, que constituye el otro ejemplo pedido. ■

Observación 19.2.7.— El concepto de permutación se corresponde con lo que en cursos anteriores nos comentaron de ser la permutación el caso en que «importaba el orden de disposición de los elementos, ninguno de éstos se repetía e intervenían necesariamente todos».

Observación 19.2.8.— Una permutación de los elementos de un conjunto finito X de n elementos es una variación de n elementos de dicho conjunto X.

Teorema 19.34
Si X tiene n elementos, el *número de permutaciones* de sus elementos es $n!$ y lo notamos $P(n)$ (o, sinónimamente, P_n).

Observación 19.2.9.— Si X tiene n elementos, el número de permutaciones de sus elementos es igual al número de variaciones de n elementos de dicho conjunto X, esto es, $P(n) = V(n, n)$.

Ejemplo 632 (PRen3)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir siete tareas distinguibles entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si ninguno de éstos puede recibir más de una?

Resolución.— Cada reparto (asignación o distribución) corresponde a una aplicación inyectiva del conjunto de tareas $\{t, t', \ldots, t''''''\}$ en el conjunto no vacío A de computadores auxiliares

$\{c_1, c_2, \ldots, c_7\}$, que también tiene cardinal 7 (inyectiva porque ningún computador auxiliar puede recibir más de una tarea); como la aplicación es inyectiva y ambos conjuntos tienen el mismo cardinal, entonces la aplicación es biyectiva, así, diremos que cada reparto es una permutación de los elementos de A; el número de posibles repartos es el número de permutaciones, por lo tanto, existen $P(7) = 7! = 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040$ formas posibles de repartir las tareas.

Observemos que $P(7) = V(7, 7)$. ■

Observación 19.2.10.— Notemos la similitud con una resolución posible del ejemplo anterior por el principio de la multiplicación ($7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ han sido las formas).

Observación 19.2.11.— Notemos también que todo ha consistido en seleccionar ordenadamente los 7 computadores auxiliares que han recibido una tarea cada uno; selección sin reemplazamiento, ya que un computador auxiliar puede ser seleccionado más de una vez (no puede recibir más de una tarea) (*cfr. infra*. cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—)..

Observación 19.2.12.— Por cierto, ¿por qué 5040 es un número bien conocido? (¿Y por qué son famosos los números naturales 0, 1, 2, 3, 6, 42, 73, 1089, 6174 y tantos otros?)

Codificación por transposición

En este tipo de codificación, el mensaje se divide en bloques de una longitud prefijada n y cada uno de estos bloques se cifra independientemente del resto según una permutación común para todos los bloques.

Por ejemplo, suponiendo el mensaje «A presurosa demanda, espaciosa respuesta» y $n = 8$, tenemos cinco bloques: «A presur», «osa dema», «nda, esp», «aciosa r» y «espuesta». Aplicando la permutación

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 1 & 4 & 5 & 7 & 2 & 0 \end{pmatrix}$$

a cada bloque, éstos, cifrados, son «rpu reAs», «aams doe», «pasd, n», «ri cosaa» y «aptsuees», es decir, el mensaje cifrado es «rou reAsaams doepasd, nri cosaaaptsuees».

Observemos que si bien se pierde la gramática de la lengua, se conservan las frecuencias de las palabras por lo que esta codificación es vulnerable a ataques con técnicas de análisis de frecuencias.

§ 19.2.3 Generación de permutaciones en orden lexicográfico

Definición 19.18.— Sean dos permutaciones σ_i y σ_j del conjunto $\{a_1, \ldots, a_n\}$. Decimos que σ_i *precede lexicográficamente* a σ_j precisamente si en la primera posición k en que difieren, el elemen-

to de σ_i es menor que el de σ_j, esto es, $(\sigma_i(a_1), \dots, \sigma_i(a_n)) \prec (\sigma_j(a_1), \dots, \sigma_j(a_n))$ si, y sólo si, $(\exists k \in \{1, \dots, n\})(\sigma_i(a_1) = \sigma_j(a_1) \wedge \sigma_i(a_2) = \sigma_j(a_2) \wedge \cdots \wedge \sigma_i(a_{k-1}) = \sigma_j(a_{k-1}) \wedge \sigma_i(a_k) < \sigma_j(a_k))$.

Parte de la idea para generar la siguiente permutación en orden lexicográfico es la siguiente.

- si $\sigma_i(a_{n-1}) < \sigma_i(a_n)$, entonces `intercambiar`$(\sigma_i(a_{n-1}), \sigma_i(a_n))$; por ejemplo, la siguiente permutación a $\langle 1, 2, 3, 4, 5, 6, 7 \rangle$ es $\langle 1, 2, 3, 4, 5, 7, 6 \rangle$;
- si $\sigma_i(a_{n-1}) > \sigma_i(a_n)$, entonces si $\sigma_i(a_{n-2}) < \sigma_i(a_{n-1})$, entonces
  - colocar $\text{mín}(\sigma_i(a_{n-1}), \sigma_i(a_n))$ en la posición $n-2$, y
  - colocar en orden creciente $\text{máx}(\sigma_i(a_{n-1}), \sigma_i(a_n))$ y a_{n-2} (el original) en las posiciones $n-1$ y n;

  por ejemplo, la siguiente permutación a $\langle 1, 2, 3, 4, 5, 7, 6 \rangle$ es $\langle 1, 2, 3, 4, 6, 5, 7 \rangle$ (como $\sigma_i(a_{n-2}) = 5 < \sigma_i(a_{n-1}) = 7$, se coloca $\text{mín}(\sigma_i(a_{n-1}), \sigma_i(a_n)) = \text{mín}(7, 6) = 6$ en la posición $n-2$ y se colocan en orden creciente $\text{máx}(\sigma_i(a_{n-1}), \sigma_i(a_n)) = \text{máx}(7, 6) = 7$ y $a_{n-2} = 5$, esto es, $\langle 5, 7 \rangle$ en las posiciones $n-1$ y n).

Actividad 19.10

Deducir el procedimiento para el caso general.

Para hallar la siguiente permutación a una dada, pudiésemos utilizar el artefacto en línea SageMath[19] y el siguiente programita en lenguaje Sage,

[19] *Cfr. supra* § 11 (pág. cii de esta edición).

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/

def siguiente_permutacion(A):
n = len(A)
if n <= 1:
        raise ValueError(”La longitud debe ser mayor que 1.”)

# Paso 1: encontrar el índice k tal que A[k] < A[k+1]
k = n - 2
while k >= 0 and A[k] >= A[k + 1]:
        k -= 1

if k < 0:
        raise ValueError(”La permutación es la última posible en orden lexicográfico.”)

# Paso 2: encontrar el índice m tal que A[m] > A[k]
m = n - 1
while A[m] <= A[k]:
        m -= 1

# Paso 3: intercambiar A[k] y A[m]
A[k], A[m] = A[m], A[k]

# Paso 4: invertir el subarreglo desde A[k+1] hasta A[n-1]
A[k+1:] = reversed(A[k+1:])

return A

# Ejemplo de utilización
A = [’1’, ’2’, ’3’, ’4’, ’5’, ’7’, ’6’]
print(”Permutación actual:”, A)
A = siguiente_permutacion(A)
print(”Siguiente permutación:”, A)
```

A continuación, mostramos la traza del algoritmo `siguiente_permutacion` para la permutación $A = \langle 1, 2, 3, 4, 5, 7, 6 \rangle$.

Paso	**Acción**
0.	$k := 6$ (inicialmente).
1.	$A[5] = 7 > A[6] = 6$, por lo tanto, $k := 5$.
2.	$A[4] = 5 < A[5] = 7$, por lo tanto, $k := 4$.
3.	$m := 6$.
4.	$A[6] = 6 > A[4] = 5$, por lo tanto, m no cambia.

5. Intercambia $A[4]$ y $A[6]$, dando $A = \langle 1, 2, 3, 4, 6, 7, 5\rangle$.
6. Invierte el orden desde $A[5]$ hasta $A[6]$, dando $A = \langle 1, 2, 3, 4, 6, 5, 7\rangle$.

§ 19.2.4 Permutación con repetición

Definición 19.19.— Una *permutación con repetición* de orden $k_0, k_1, \cdots, k_{p-1}$ de los elementos de un conjunto Y de p elementos, es cualquier aplicación sobreyectiva de un conjunto X de $k_0 + k_1 + \cdots + k_{p-1}$ elementos en Y, sujeta a las condiciones siguientes: k_0 elementos de X tienen la misma imagen $y_0 \in Y$, k_1 elementos de X tienen la misma imagen $y_1 \in Y, \dots, k_{p-1}$ elementos de X tienen la misma imagen $y_{p-1} \in Y$, además $\forall i, j \in \{0, 1, \dots, p-1\}, i \neq j, y_i \neq y_j$.

Ejemplo 633

Dados los conjuntos $X = \{a, b, c, d, e\}$ e $Y = \{x, y, z\}$, proporcionemos dos ejemplos de permutación con repetición de orden $3, 1, 1$ de los elementos de Y.

Resolución.— Dados los conjuntos $X = \{a, b, c, d, e\}$ e $Y = \{x, y, z\}$, un ejemplo de permutación con repetición de orden $3, 1, 1$ de los elementos de Y es $a \longmapsto x, b \longmapsto x, c \longmapsto x, d \longmapsto y, e \longmapsto z$, que abreviamos con la tupla $\langle x, x, x, y, z\rangle$; esta permutación con repetición es una aplicación distinta de, por ejemplo, $a \longmapsto x, b \longmapsto y, c \longmapsto x, d \longmapsto z, e \longmapsto x$, abreviadamente, $\langle x, y, x, z, x\rangle$, que constituye el otro ejemplo pedido. ■

Observación 19.2.13.— Si bien representamos mediante una tupla tanto la variación con repetición como la permutación con repetición, en una tupla correspondiente a esta última deben estar todos los elementos del conjunto Y (debido a la sobreyectividad).

Observación 19.2.14.— El concepto de permutación con repetición se corresponde con lo que en cursos anteriores nos comentaron de ser la permutación con repetición el caso en que «importaba el orden de disposición de los elementos, algunos de éstos se repetían e intervenían necesariamente todos».

Teorema 19.35
El *número de permutaciones con repetición* es igual a $\binom{k_0 + k_1 + \cdots + k_{p-1}}{k_0, k_1, \dots, k_{p-1}}$ y lo notamos $PR(k_0, k_1, \dots, k_{p-1})$ —o, sinónimamente, $PR_{k_0,k_1,\dots,k_{p-1}}$ (también, si $n = k_0 + k_1 + \cdots + k_{p-1}$: $C_{n,(k_0,k_1,\dots,k_{p-1})}$, $C^n_{(k_0,k_1,\dots,k_{p-1})}$, ${}_nC_{(k_0,k_1,\dots,k_{p-1})}$, ${}^nC_{(k_0,k_1,\dots,k_{p-1})}$ o $C_n^{(k_0,k_1,\dots,k_{p-1})}$)—.

Observación 19.2.15.— Tanto si interpretamos una permutación con repetición $PR(k_0, k_1, \dots, k_{p-1})$ como

0. una forma de disponer k_0 objetos indistinguibles de tipo 0, k_1 objetos indistinguibles de tipo 1, ..., k_{p-1} objetos indistinguibles de tipo $p-1$, como si la interpretamos
1. como una forma de disponer $k_0+k_1+\cdots+k_{p-1}$ objetos distinguibles en p recipientes de manera que el recipiente i tenga k_i objetos,

entonces el *número de permutaciones con repetición* es el número de formas de disponerlos.

Ejemplo 634

Sea $\Sigma = \{a, b, c\}$; ¿cuántas palabras de Σ^* de longitud diez están formadas exactamente por cuatro aes, tres bes y tres ces?

Resolución.— Pudiésemos ver el alfabeto Σ como el conjunto subyacente del multiconjunto $M = \{a, a, a, a, b, b, b, c, c, c\}$, de interés para esta situación. Cada palabra corresponde a una aplicación sobreyectiva del conjunto de diez posiciones de letras de la palabra de diez letras $P = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\}$ en Σ, por lo que cada palabra es una permutación con repetición de orden 4, 3, 3, de donde el número de palabras es el número de permutaciones con repetición; por lo tanto, existen $PR(4, 3, 3) = (4+3+3)!/(4!\cdot 3!\cdot 3!) = 4200$ palabras con tales características. ■

Observación 19.2.16.— Éste ha sido un ejemplo de la observación 19.2.15.0 (pág. 1164 de esta edición), donde los objetos indistinguibles de tipo 0 son las aes, los de tipo 1, las bes, y los de tipo 2, las ces, siendo $k_0 = 4$ y $k_1 = k_2 = 3$.

Ejemplo 635 (PRen4)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir siete tareas, tres indistinguibles y cuatro distinguibles de esas tres y distinguibles también entre sí, entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si cada uno de éstos recibe una tarea y sólo una?

Resolución.— Sea el multiconjunto de tareas $M = \{\{r, r, r, s, t, u, v\}\}$ (llamémoslas, por ejemplo, así) y sea $X = \{r, s, t, u, v\}$ su conjunto subyacente. Cada reparto corresponde a una aplicación sobreyectiva del conjunto de computadores $C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7\}$ en X, aplicación que representamos por una tupla de siete componentes (por ejemplo, $\langle r, t, r, v, r, s, u\rangle$, que asigna r a c_1, c_3 y c_5, s a c_6, t a c_2, u a c_7 y v a c_4). Así, diremos que cada reparto es una permutación con repetición de orden 3, 1, 1, 1, 1; entonces el número de posibles repartos es el número de permutaciones con repetición; por lo tanto, existen $PR(3, 1, 1, 1, 1) = (3+1+1+1+1)!/(3!\cdot 1!\cdot 1!\cdot 1!\cdot 1!) = 7!/3! = 7\cdot 6\cdot 5\cdot 4 = 840$ formas posibles de repartir las tareas. ■

Observación 19.2.17.— Éste ha sido un ejemplo de la observación 19.2.15.1 (pág. 1164 de esta edición), donde los objetos distinguibles son los siete computadores auxiliares y los recipientes son las letras r, s, t, u, v, siendo $k_0 = 3$ y $k_1 = k_2 = k_3 = k_4 = 1$.

Observación 19.2.18.— El resultado coincide con $V(7,4) = 7^{\underline{4}} = 7 \cdot 6 \cdot 5 \cdot 4$, esto es, con seleccionar ordenadamente los cuatro computadores auxiliares que han recibido una tarea distinguible cada uno —selección sin reemplazamiento, ya que ninguno de estos cuatro computadores auxiliares puede ser seleccionado más de una vez (ninguno puede recibir más de una tarea)— (a cada uno de los tres computadores auxiliares restantes se le asigna cualquiera de las tareas indistinguibles).

En realidad, lo que hemos hecho en esta observación es reducir el problema original, llamémoslo A, al problema, digamos B, de reparto de cuatro tareas distinguibles entre siete computadores auxiliares de tal forma que ninguno puede recibir más de una tarea —hemos reducido PRen4 a PRen1—. La solución del problema B existe —*cfr. supra* ejemplo 626 (pág. 1155 de esta edición)— y proporciona una solución para el problema A caso de que éste la tenga.

Actividad 19.11

Realicemos una demostración combinatoria, por codificación de subconjuntos como aplicaciones, para un conjunto X finito, de que el cardinal de su conjunto potencia es $2^{|X|}$.

[Cubit 135].

§ 19.2.5 Combinación

Definición 19.20.— Una *combinación* de k elementos de un conjunto no vacío X es cualquier subconjunto de X de k elementos.

Ejemplo 636

Proporcionemos un ejemplo de combinación de tres elementos del conjunto $X = \{a, b, c, d, e\}$.

Resolución.— Dado el conjunto $X = \{a, b, c, d, e\}$, un ejemplo de combinación de tres elementos de X es el subconjunto $\{a, c, d\}$; esta combinación es el mismo subconjunto que, por ejemplo, $\{d, a, c\}$. ■

Observación 19.2.19.— El concepto de combinación se corresponde con lo que en cursos anteriores nos comentaron de ser la combinación el caso en que «no importa el orden de disposición de los elementos, ninguno de éstos se repite y no intervienen necesariamente todos».

Teorema 19.36

Si X tiene n elementos, el *número de combinaciones* de k elementos ($k \leq n$) es igual a $\binom{n}{k}$, esto es, a $n!/(k!(n-k)!)$, y lo notamos $C(n,k)$ —o, sinónimamente, $C_{n,k}$, C_k^n, ${}_nC_k$, ${}^nC_k$ o C_n^k—.

Teorema 19.37

Se satisface la *interrelación*

$$V(n,k) = P(k) \cdot C(n,k).$$

Ejemplo 637

¿Cuántas palabras binarias (base 2) de longitud n con k ceros existen?

a. n^k.

b. $(n-k)! \cdot k!$.

c. $(n-k)! + k!$.

d. $\binom{n}{n-k}$.

[TT], [EFE 3.7.2024:10] (tipo test).

Resolución.— Esto es tanto como preguntarnos ¿de cuántas formas podemos colocar k ceros en n posiciones?, lo cual equivale a preguntarnos ¿de cuántas formas podemos elegir k posiciones de un total de n?, que si en vez de posiciones hablamos de elementos de un conjunto, sería: ¿cuántos subconjuntos de k elementos de un conjunto de n elementos existen? Recordemos que una combinación de k elementos de un conjunto no vacío X es cualquier subconjunto de X de k elementos y que si X tiene n elementos, el número de combinaciones de k elementos ($k \leq n$) es $\binom{n}{k}$, es decir, $\binom{n}{n-k}$.

Solución.— Opción d. ■

Ejemplo 638 (PRen5)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir tres tareas indistinguibles entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si ninguno de éstos puede recibir más de una?

Resolución.— Si un computador auxiliar recibe una tarea, al ser las tres indistinguibles, da igual qué tarea ha recibido, esto es, cada reparto corresponde a una elección de tres computadores auxiliares entre los siete sin importar el orden, pues las tres tareas son indistinguibles (carece de sentido ordenar ttt) y sin reemplazamiento, ya que un computador auxiliar puede ser elegido sólo una vez (no puede recibir más de una tarea), en otras palabras, estamos eligiendo un subconjunto de tres elementos de un conjunto de siete; así, diremos que cada reparto es una combinación de tres elementos de un conjunto no vacío de siete elementos, concretamente del conjunto $C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7\}$ de siete computadores auxiliares. El número de posibles repartos es el número de combinaciones,

por lo tanto, existen $C(7,3) = 7!/(3! \cdot (7-3)!) = 35$ formas posibles en que c_0 puede repartir las tareas. ■

Observación 19.2.20.— Este valor, 35, también es el número de permutaciones con repetición de orden 3, 4 de los elementos de un conjunto Y de dos elementos, digamos $\{y_0, y_1\}$, esto es, el número de aplicaciones sobreyectivas de un conjunto X de $3+4$ elementos en Y, en las que en cada una, tres elementos de X tienen por imagen y_0 y cuatro elementos de X tienen por imagen y_1.

El siguiente ejemplo muestra un enunciado que corresponde a esta observación.

Ejemplo 639 (PRen5bis)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir tres primeras tareas indistinguibles y cuatro segundas tareas indistinguibles —pero distinguibles de las tres anteriores— entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si ninguno de éstos puede recibir más de una?

Resolución.— Cada reparto es una permutación con repetición de orden 3, 4 de los elementos de un conjunto de dos elementos, digamos $\{0,1\}$, esto es, una aplicación sobreyectiva del conjunto $C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7\}$ de siete computadores auxiliares en $\{0,1\}$ tal que tres elementos de C tienen por imagen 0 y cuatro elementos de C tienen por imagen 1. El número de posibles repartos es el número de permutaciones con repetición, esto es, existen $PR(3,4) = (3+4)!/(3! \cdot 4!) = 35$ formas posibles en que c_0 puede repartir las tareas. ■

Observación 19.2.21.— Pudiésemos resolver este ejemplo por combinaciones, obteniendo, bien $C(7,3)$ si partiésemos de las tres indistinguibles (como en PRen5), bien $C(7,4)$ si partiésemos de las cuatro indistinguibles; en cualquier caso, $C(7,3) = C(7,4) = PR(3,4) = 35$.

Observación 19.2.22.— En cualquier caso, éste es un ejemplo de la única *distribución no simple* que veremos en estas notas. Para saber más sobre ella, *vid. infra* § 19.5 (pág. 1235 de esta edición).

Actividad 19.12

Siendo $n = k_0 + k_1 + \cdots + k_{p-1}$, demostremos que

$$PR(k_0, k_1, \ldots, k_{p-1}) = \binom{n}{k_0}\binom{n-k_0}{k_1}\binom{n-k_0-k_1}{k_2}\cdots\binom{k_{p-2}+k_{p-1}}{k_{p-2}}\binom{k_{p-1}}{k_{p-1}}.$$

Ejemplo 640 (PRen6)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir siete tareas, tres indistinguibles y cuatro distinguibles de esas tres y distinguibles también entre sí, entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si algunos de éstos pueden recibir dos o más tareas distinguibles y ninguno dos o más tareas indistinguibles? Para calcularlas: 0.º, formalicemos la situación según el principio de la multiplicación, el suceso y sus fases; 1.º, razonemos de cuántas formas puede realizarse cada una de las fases, y 2.º, finalmente, apliquemos el principio de la multiplicación.

[EFE 22.6.2022:8].

Resolución.— Nuestra estrategia de resolución comienza por calcular el número de repartos posibles de las cuatro tareas distinguibles —y, por ahora, como poder quedar, quedarán seguro computadores auxiliares sin recibir tarea—, para después determinar el número de repartos de las tareas indistinguibles y finalmente agregarlos mediante el principio de la multiplicación.

0.°, *Formalización del principio de la multiplicación: del suceso y sus fases.*

El suceso

$S \leftrightharpoons$ se reparten siete tareas, tres indistinguibles y cuatro distinguibles a esas tres y distinguibles también entre sí, entre siete computadores auxiliares, pudiendo algunos de éstos recibir dos o más tareas distinguibles y ninguno dos o más tareas indistinguibles,

sucede en las dos fases sucesivas e independientes consecutivamente,

fase 0 $\leftrightharpoons$ se reparten cuatro tareas distinguibles entre siete computadores auxiliares, pudiendo algunos de éstos recibir dos o más tareas,

fase 1 $\leftrightharpoons$ se reparten tres tareas indistinguibles entre siete computadores auxiliares, no pudiendo ninguno de éstos recibir dos o más tareas.

1.°, *De las formas de realizar las fases.*

a. *Resolución de la fase* 0.

Decir «si algunos de éstos pueden recibir dos o más tareas distinguibles» no aporta información alguna, es como no decir nada.

Como cada computador auxiliar puede recibir más de una tarea, cada reparto de las cuatro tareas distinguibles corresponde a una aplicación cualquiera —sin ninguna condición— del conjunto de tareas $\{1, 2, 3, 4\}$ en el conjunto no vacío A de computadores auxiliares; así, diremos que cada reparto de las cuatro tareas distinguibles es una variación con repeti-

ción de cuatro elementos de A, esto es, el número de posibles repartos de las cuatro tareas distinguibles es el número de variaciones con repetición, por lo tanto, existen —*cfr. supra* ejemplo 629 (pág. 1157 de esta edición)—

$$\begin{aligned} VR(7,4) &= 7^4 \\ &= 7 \cdot 7 \cdot 7 \cdot 7 \\ &= 2401 \end{aligned}$$

formas posibles de repartir las cuatro tareas distinguibles.

b. *Resolución de la fase* 1.

Ahora, pensemos en las tres tareas indistinguibles. Ningún computador auxiliar puede recibir dos tareas indistinguibles, por lo que, en este caso nos interesa el número de formas de repartir las tres tareas indistinguibles entre los siete computadores auxiliares si ninguno de éstos puede recibir más de una tarea. Pues bien, si un computador auxiliar recibe una tarea, al ser las tres indistinguibles, da igual qué tarea ha recibido, esto es, cada reparto (asignación o distribución) corresponde a una selección de tres computadores auxiliares entre los siete sin importar el orden —el orden no importa porque las tres tareas son indistinguibles; no es posible ordenar ttt— y sin reemplazamiento, ya que un computador auxiliar puede ser seleccionado sólo una vez —no puede recibir más de una tarea—; en otras palabras, se está seleccionando, en tales condiciones, un subconjunto de tres elementos de un conjunto de siete, así, diremos que cada reparto es una combinación de tres elementos de un conjunto no vacío A de siete elementos, esto es, el número de posibles repartos es el número de combinaciones, por lo tanto, existen —*cfr. supra* ejemplo 638 (pág. 1166 de esta edición)—

$$\begin{aligned} C(7,3) &= \frac{7!}{3! \cdot (7-3)!} \\ &= 35 \end{aligned}$$

formas posibles de repartir las tareas.

2.°, *Aplicación del principio de la multiplicación*.

Entonces, el suceso S se ha resuelto en dos fases sucesivas, independientes consecutivamente, por lo que por el principio de la multiplicación, el número de formas de repartir las tareas es

$$\begin{aligned} VR(7,4) \cdot C(7,3) &= 2401 \cdot 35 \\ &= 84\,035. \end{aligned}$$

Solución.— De 84 035 formas. ■

Ejemplo 641

Utilicemos razonadamente el principio de la adición para calcular el número de subconjuntos de $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ que tienen un número primo de elementos. Para ello: 0.°, formalicemos la situación según el principio de la adición; 1.°, razonemos de cuántas formas sucede cada uno de los sucesos intervinientes, y 2.°, finalmente, apliquemos el principio de la adición.

[PEP 2016–2017:1], [EFE 19.1.2023:7].

Resolución.— Veamos.

0.°, *Formalización del principio de la adición*.

Para poder aplicar el principio de la adición debemos definir sucesos incompatibles dos a dos. Para ello, observemos que se trata de conjuntos y no de multiconjuntos, por lo que no se pueden repetir los elementos. Por esto, las únicas posibilidades de cardinalidad prima para ellos son los números primos menores o iguales que diez (el cardinal de D), a saber, 2, 3, 5 y 7.

De este modo, pudiésemos hablar de los sucesos

$$\begin{aligned} S_2 &\leftrightharpoons \text{ser un subconjunto de exactamente dos elementos de } D, \\ S_3 &\leftrightharpoons \text{ser un subconjunto de exactamente tres elementos de } D, \\ S_5 &\leftrightharpoons \text{ser un subconjunto de exactamente cinco elementos de } D, \\ S_7 &\leftrightharpoons \text{ser un subconjunto de exactamente siete elementos de } D. \end{aligned}$$

que son incompatibles dos a dos, puesto que deben tener exactamente el número de elementos que dice cada uno.

1.°, *De las formas de suceder los sucesos*.

El número total de subconjuntos de k elementos de un conjunto de n elementos viene dado por el número de combinaciones de n elementos tomados de k en k, $C(n, k)$. De aquí que:

- el suceso S_2 sucede de $C(10, 2)$ formas distintas;
- el suceso S_3 sucede de $C(10, 3)$ formas distintas;
- el suceso S_5 sucede de $C(10, 5)$ formas distintas, y
- el suceso S_7 sucede de $C(10, 7)$ formas distintas.

2.°, *Aplicación del principio de la adición*.

Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_2 \cup S_3 \cup S_5 \cup S_7$. Como hemos dicho ya, son sucesos incompatibles dos a dos —por tener exactamente el número de elementos que indica cada subíndice—, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

$$\begin{aligned}\#(S_2 \cup S_3 \cup S_5 \cup S_7) &= \#S_2 + \#S_3 + \#S_5 + \#S_7 \\ &= \binom{10}{2} + \binom{10}{3} + \binom{10}{5} + \binom{10}{7} \\ &= \frac{10!}{2! \cdot 8!} \cdot \frac{10!}{3! \cdot 7!} \cdot \frac{10!}{5! \cdot 5!} \cdot \frac{10!}{7! \cdot 3!} \\ &= 537.\end{aligned}$$

Solución.— El conjunto $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ tiene 537 subconjuntos con un número primo de elementos. ■

Observación 19.2.23.— En la formulación del principio con conjuntos disjuntos dos a dos, éstos son $S_i = \{x : x \text{ es subconjunto de exactamente } i \text{ elementos de } D\}$ y sus cardinales,

$$|S_i| = \binom{n}{i}.$$

Ejemplo 642

Por cierto, del conjunto D del ejemplo anterior, ¿cuántos subconjuntos suyos hay cuyos elementos son todos números primos?

Resolución.— Siendo $P = \{2, 3, 5, 7\}$, lo que queremos hallar es en realidad el número de subconjuntos no vacíos de P, esto es, restando uno (el conjunto vacío) al número total de subconjuntos de P:

$$\begin{aligned}|2^P| - 1 &= 2^{|P|} - 1 \\ &= 2^4 - 1 \\ &= 15.\end{aligned}$$

Solución.— Hay 15 subconjuntos de D cuyos elementos son todos números primos. ■

Ejemplo 643

Colocamos aleatoriamente los números $\{1, 2, 3, \dots, 8\}$ en forma de matriz 2×4.

0. ¿Es posible asegurar que alguna fila contiene al menos dos múltiplos de dos?
1. ¿Cuántas colocaciones existen en las que en cada fila el elemento que inicia la fila es el mínimo de la fila?

Resolución.—

0. Hay cuatro múltiplos de dos entre esos números, a saber, 2, 4, 6 y 8; aplicando el principio restringido de los cajones de Dirichlet, como $k = 4$ objetos (los cuatro múltiplos de dos) se distribuyen en $n = 2$ cajones (las dos filas) y $2 = n < k = 4$, entonces hay al menos un cajón que recibe al menos dos objetos, esto es, hay al menos una fila que contiene al menos dos múltiplos de dos.

1. Sea el suceso

$S \risingdotseq$ ser una matriz 2×4 en la que en cada fila el elemento que la inicia es el mínimo de la fila.

Dicho suceso ocurre en dos fases independientes consecutivamente,

$S_0 \risingdotseq$ la colocación en la fila cero de cuatro números, elegidos de ocho, de tal forma que el elemento que la inicia sea el mínimo de la fila;

$S_1 \risingdotseq$ la colocación en la fila uno de cuatro números dados, de tal forma que el elemento que la inicia sea el mínimo de la fila.

en realidad, descompuestas en tres subfases cada una:

$S_0^4 \risingdotseq$ la elección de cuatro números para la fila cero;

$S_{00} \risingdotseq$ la colocación del menor de estos cuatro números en la posición cero de la fila cero;

$S_{01} \risingdotseq$ la colocación del resto, tres números, en las demás posiciones, tres, de la fila cero;

$S_1^4 \risingdotseq$ la elección de los cuatro números restantes;

$S_{10} \risingdotseq$ la colocación del menor de estos cuatro números en la posición cero de la fila uno;

$S_{11} \risingdotseq$ la colocación del resto, tres números, en las demás posiciones, tres, de la fila uno.

Las formas de realizar estas subfases son (pensemos por qué):

$\#S_0^4 = C(8, 4) = 70;$

$\#S_{00} = 1;$

$\#S_{01} = P(3) = 3!;$

$\#S_1^4 = C(4,4) = 1;$

$\#S_{10} = 1;$

$\#S_{11} = P(3) = 3!.$

Aplicando el principio de la multiplicación, tenemos que el número de formas en que sucede S es el producto de las formas en que pueden realizarse las subfases, esto es, $\#S = 70 \cdot 1 \cdot 6 \cdot 1 \cdot 1 \cdot 6 = 2520$. ■

Ejemplo 644

Consideremos las palabras hexadecimales de longitud 4, esto es, palabras con la forma $n_0n_1n_2n_3$, con $n_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}\}$. De entre ellas, ¿cuántas hay que contengan A y B —esto es, que algún n_i sea A y algún n_i sea B— y tales que ningún n_i pertenezca a $\{0, 1, 2, 3, 4, 5, 6\}$? (Por ejemplo, 7BEA, A98B y ABBA son tres de tales palabras, pero A9FE y A80B no lo son).

a. 770.

b. 997.

c. 1631.

d. 4032.

[TT], [EFE 3.7.2024:11] (tipo test).

Resolución.— Sea J el conjunto de palabras de longitud 4 que no contienen ningún carácter de $\{0, 1, 2, 3, 4, 5, 6\}$, esto es, el conjunto de aquéllas que pueden formarse con los elementos del conjunto $K = \{7, 8, 9, \mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{E}, \mathrm{F}\}$; se tiene que $|J| = 9^4$ (el número de variaciones con repetición de 4 elementos del conjunto K).

Debemos calcular el número de palabras de J que contienen A y B. Para ello utilizaremos el principio del complementario. Lo contrario a contener A y B es no contener A o no contener B (por la ley de De Morgan). Consideramos los subconjuntos de J:

- $J_{\not{A}}$, el de las palabras de J que no contienen A, cuyo cardinal es 8^4 (el número de variaciones con repetición de 4 elementos del conjunto $K - \{\mathrm{A}\}$);
- $J_{\not{B}}$, el de las palabras de J que no contienen B, cuyo cardinal también es 8^4 (el número de variaciones con repetición de 4 elementos del conjunto $K - \{\mathrm{B}\}$);
- $J_{\not{A}} \cap J_{\not{B}}$ (subconjunto intersección de $J_{\not{A}}$ y $J_{\not{B}}$), el de las palabras de J que no contienen ni A ni B, cuyo cardinal es 7^4 (el número de variaciones con repetición de 4 elementos del conjunto $K - \{\mathrm{A}, \mathrm{B}\}$);
- $J_{\not{A}} \cup J_{\not{B}}$ (subconjunto unión de $J_{\not{A}}$ y $J_{\not{B}}$), el de las palabras de J que no contienen A o no contienen B, cuyo cardinal es —por el principio de inclusión-exclusión— $|J_{\not{A}} \cup J_{\not{B}}| = |J_{\not{A}}| + |J_{\not{B}}| - |J_{\not{A}} \cap J_{\not{B}}| = 8^4 + 8^4 - 7^4 = 4096 + 4096 - 2401 = 5791$, y
- $J_{\mathrm{A,B}}$, el de las palabras de J que contienen A y B (cuyo cardinal hemos de hallar).

Como $J - J_{\mathrm{A,B}} = J_{\not{A}} \cup J_{\not{B}}$ (lo contrario a contener A y B es no contener A o no contener B), entonces, por el principio del complementario, $|J_{\mathrm{A,B}}| = |J| - |J - J_{\mathrm{A,B}}| = |J| - |J_{\not{A}} \cup J_{\not{B}}| = 9^4 - 5791 = 6561 - 5791 = 770$.

Solución.— Opción a. ■

. . . .

Una *codificación como palabra numérica* puede ayudar a resolver cuestiones. Por ejemplo, ¿pudiésemos utilizar una codificación en palabras binarias para responder a la pregunta del siguiente ejemplo?

. . . .

Ejemplo 645

De una fila de siete personas, ¿de cuántas formas es posible elegir tres de forma que ningunas dos de las elegidas estuviesen en posiciones seguidas en la fila?

[Cubit 136].

Resolución.— Codificamos cada elección como una palabra binaria donde cero significa no elegida y uno sí elegida. Entonces, una pregunta equivalente a la inicial es

> ¿Cuántas palabras binarias de longitud siete, con $7 - 3 = 4$ ceros y tres unos, existen que no contengan dos unos consecutivos?

Para descubrir cuántas son pensemos en cómo construir una de tales palabras. Pues bien, como hay $7 - 3 = 4$ ceros, hay cinco posiciones donde situar los tres unos,

$$\square\, 0\, \square\, 0\, \square\, 0\, \square\, 0\, \square$$

La pregunta inicial se reduce a:

> ¿De cuántas formas es posible colocar tres unos en cinco posiciones?

Siendo $\{p_0, p_1, p_2, p_3, p_4\}$ las cinco posiciones, colocar unos en las posiciones, por ejemplo, 1, 2 y 4, significa la extracción del subconjunto $\{p_1, p_2, p_4\}$, esto es cada colocación es una combinación de tres elementos de un conjunto de cinco elementos. Por lo tanto, el número de colocaciones es el número de combinaciones de tres elementos de un conjunto de cinco, esto es, $C(5, 3) = 10$. ■

Observación 19.2.24.— En el ejemplo anterior, $C(5, 3) = C(4 + 1, 7 - 4)$, siendo 7 la longitud de la palabra y 4 el número de ceros.

Nim, codificación binaria y Nathan (X+Y —A Brilliant Young Mind—)

Nim, un antiguo juego con piezas distribuidas en filas, que clásicamente juegan dos personas con una única regla, a saber, en cada turno, poder retirar cuantas piezas quiera de una única fila, ganando el juego quien retire la última de todas.

□□□□□□□
□□□□□
□□□□
□□□
□□□

Como es norma en los *juegos no cooperativos* (*vid. v. gr.* https://es.wikipedia.org/-wiki/Juego_no_cooperativo), quienes juegan persiguen definir una *estrategia ganadora* (*vid. v. gr.* https://en.wikipedia.org/wiki/Winning_strategy).

En esta forma de jugar Nim, puede demostrarse que existen posiciones ganadoras y perdedoras y que siempre es posible pasar de unas a otras.

Convirtiendo el número de piezas de cada fila a binario, puede demostrarse que las posiciones ganadoras son aquellas que tienen un número par de unos en cada columna. Por ejemplo, esta conversión en el caso anterior es

1 1 1 (7 piezas)
1 0 1 (5 piezas)
1 0 0 (4 piezas)
0 1 1 (3 piezas)
0 1 1 (3 piezas)

Una posición perdedora puede transformarse en ganadora; por ejemplo, la situación anterior podría transformarse en ganadora retirando 6 piezas de la primera fila, ya que entonces quedaría

0 0 1 (1 pieza)
1 0 1 (5 piezas)
1 0 0 (4 piezas)
0 1 1 (3 piezas)
0 1 1 (3 piezas)

Observemos que, en particular, la posición final —ninguna pieza en ninguna fila— es ganadora.

Pudiésemos aprender mucho más sobre Nim y sus múltiples variantes en el artículo correspondiente de Wikipedia (https://en.wikipedia.org/wiki/Nim).

Muchas demostraciones en combinatoria son posibles gracias a la codificación binaria/ternaria/… de la información. Por otra parte, pudiésemos ver esta escena de la película *X+Y* dirigida por Morgan Matthews, distribuida en los Estados Unidos como *A Brilliant Young Mind* (2014); es recomendable que atendamos al enunciado de

la cuestión propuesta en la escena y tratemos de resolverla primero; en cualquier caso, también es recomendable estudiar la resolución que se muestra en la película: escena en inglés (https://www.youtube.com/watch?v=mYAahN1G8Y8); la misma escena, subtitulada en español (https://www.youtube.com/watch?v=A_-gDrXy6V0); la misma escena, doblada a español (https://www.youtube.com/watch?v=ZnhHpr_ipgE).

Lo cierto es que es posible generalizar la demostración del ejemplo 645 (pág. 1174 de esta edición) y, por lo tanto, la observación 19.2.24 (pág. 1174 de esta edición), y obtener el siguiente teorema.

Teorema 19.38
El número de palabras binarias de longitud n con exactamente k ceros y $n-k$ unos es $C(n,k)$ y el número de ellas que no contienen dos unos consecutivos es $C(k+1, n-k)$.

Observación 19.2.25.— Si $k+1 < n-k$, entonces $C(k+1, n-k) = 0$ (por ejemplo, no existe ninguna palabra binaria de longitud diez con exactamente cuatro ceros y seis unos sin dos unos consecutivos).

Observación 19.2.26.— ¿Cuántas palabras binarias de longitud n contienen exactamente k unos? Si bien por el teorema anterior sabemos que la respuesta es $C(n,k)$, resulta interesante otra vía: preguntarnos esto equivale a contar el número de funciones de un conjunto de n elementos en $\{0,1\}$ que toman el valor 1 exactamente k veces, en otras palabras, debemos contar el número de funciones características de un conjunto de cardinal k, lo cual es, exactamente, el número de subconjuntos de k elementos del conjunto de n elementos.

Ejemplo 646

¿Cuántas palabras binarias de longitud siete existen que no contengan dos unos consecutivos?

Resolución.— El número de palabras binarias de longitud siete es $2^7 = 128$, entonces, de ellas, ¿cuántas no contienen dos unos consecutivos?

Apliquemos el principio de la adición.

0.°, *Formalización del principio de la adición: sucesos.*

Sea el suceso

$S \risingdotseq$ ser una palabra binaria de longitud siete que no contiene dos unos consecutivos,

suceso que es la unión de los sucesos

$S_k \leftrightharpoons$ ser una palabra binaria de longitud siete con k ceros y $7-k$ unos que no contiene dos unos consecutivos,

para $0 \leq k < 8$, sucesos que son trivialmente incompatibles dos a dos.

1.°, *De las formas de suceder los sucesos S_k.*

El suceso S_k sucede de $C(k+1, 7-k)$ formas distintas. En efecto, el teorema 19.38 (pág. 1176 de esta edición) establece que el número de palabras binarias de longitud n con exactamente k ceros y $n-k$ unos es $C(n,k)$ y el número de ellas que no contienen dos unos consecutivos es $C(k+1, n-k)$. Por tanto, según esto, para cada caso posible hay $C(k+1, n-k)$ palabras binarias de longitud n con exactamente k ceros y $n-k$ unos y que no contienen dos unos consecutivos. En este ejemplo, como $n=7$, se tiene el siguiente cuadro.

k ceros	$n-k$ unos	$C(k+1, n-k)$
7 ceros	0 unos	$C(7+1, 0) = 1$
6 ceros	1 unos	$C(6+1, 1) = 7$
5 ceros	2 unos	$C(5+1, 2) = 15$
4 ceros	3 unos	$C(4+1, 3) = 10$
3 ceros	4 unos	$C(3+1, 4) = 1$
2 ceros	5 unos	$C(2+1, 5) = 0$
1 ceros	6 unos	$C(1+1, 6) = 0$
0 ceros	7 unos	$C(0+1, 7) = 0$

2.°, *Aplicación del principio de la adición.*

Por el principio de la adición, el número de formas en que sucede el suceso $S = S_0 \cup S_1 \cup \ldots \cup S_7$ es la suma de los números de formas en que suceden los sucesos $S_0, S_1, \ldots, S_7$, esto es, $1+7+15+10+1+0+0+0 = 34$.

Solución.— Existen 34 palabras binarias de longitud siete que no contienen dos unos consecutivos. ■

Ejemplo 647

¿Cuántas palabras binarias de longitud n existen que no contengan dos unos consecutivos?

Resolución.— Un procedimiento similar nos permite responder a la pregunta general.

De hecho, pudiésemos compactar la suma anterior utilizando la notación sigma; para ello, cambiamos la forma de los sumandos usando la igualdad

$$\binom{k+1}{n-k} = \binom{(n-k)+1}{n-(n-k)}$$

$$= \binom{(n-k)+1}{k},$$

de donde

$$\begin{aligned}
\sum_{k=0}^{7} \binom{(7-k)+1}{k} &= 1+7+15+10+1+0+0+0 \\
&= \binom{(7-0)+1}{0} + \binom{(7-1)+1}{1} + \binom{(7-2)+1}{2} \\
&\qquad + \binom{(7-3)+1}{3} + \binom{(7-4)+1}{4} \\
&= \binom{7+1}{0} + \binom{7}{1} + \binom{7-1}{2} + \binom{7-2}{3} + \binom{7-3}{4} \\
&= 34.
\end{aligned}$$

Sabemos que si $i < j$, $C(i,j) = 0$. Así, como, por un lado, $(n - \lceil n/2 \rceil) + 1 > \lceil n/2 \rceil$ si n es par y $(n - \lceil n/2 \rceil) + 1 = \lceil n/2 \rceil$ si n es impar, y, por otro, $(n - (\lceil n/2 \rceil + 1)) + 1 < \lceil n/2 \rceil + 1$, para todo $n \in \mathbb{Z}^+$, entonces, si estuviésemos hablando de palabras binarias de longitud n, del total de 2^n palabras, las que no tendrían dos unos consecutivos serían

$$\binom{(n-0)+1}{0} + \binom{(n-1)+1}{1} + \cdots + \binom{(n - \lceil \frac{n}{2} \rceil)+1}{\lceil \frac{n}{2} \rceil}$$

esto es,

$$\binom{n+1}{0} + \binom{n}{1} + \cdots + \binom{n - \lceil \frac{n}{2} \rceil + 1}{\lceil \frac{n}{2} \rceil}$$

Ésta es la solución buscada. ■

§ 19.2.6 Generación de combinaciones

Sea el conjunto de n elementos, $\{0, 1, \ldots, n\}$. Para hallar la siguiente combinación a una dada, pudiésemos utilizar el artefacto en línea SageMath[20] y el siguiente programita en lenguaje Sage,

```
# Ejecutar en: Sage Cell Server — https://sagecell.sagemath.org/

def siguiente_combinacion(n, k, X):
"""
Devuelve la siguiente combinación en orden lexicográfico.
X: lista de longitud k, que representa una combinación de k elementos
"""

if k >= n or k < 1:
        raise ValueError("Debe cumplirse 1 ≤ k < n.")
```

[20] *Cfr. supra* § 11 (pág. cii de esta edición).

```
    j = 0
    while j < k and X[k - 1 - j] == n - j:
        j += 1

    if j == k:
        raise ValueError("Es la última combinación.")

    X[k - 1 - j] += 1
    for i in range(k - j, k):
        X[i] = X[i - 1] + 1

    return X

# ejemplo de utilización
n = 6
k = 4
X = [1, 2, 0, 6]
print("Combinación actual:", X)
print("Siguiente combinación:", siguiente_combinacion(n, k, X[:]))
```

Actividad 19.13

Tomando $n = 6$, $k = 4$ y $X = \{1, 2, 0, 6\}$, el algoritmo `siguiente_combinacion` da como resultado la combinación $\{1, 2, 1, 2\}$; mostremos la traza.

§ 19.2.7 Combinación con repetición

Definición 19.21.— Una *combinación con repetición* de orden k de elementos de un conjunto no vacío X es un multiconjunto de elementos de X de cardinalidad k.

Ejemplo 648

Proporcionemos un ejemplo de combinación con repetición de orden cuatro del conjunto $X = \{a, b, c, d, e\}$.

Resolución.— Dado el conjunto $X = \{a, b, c, d, e\}$, un ejemplo de combinación con repetición de orden cuatro de X es el submulticonjunto $\{\{a, c, d, c\}\}$; esta combinación con repetición es el mismo submulticonjunto que, por ejemplo, $\{\{d, a, c, c\}\}$. ■

Observación 19.2.27.— El concepto de combinación con repetición se corresponde con lo que en cursos anteriores nos comentaron de ser la combinación con repetición el caso en que «no importa el orden de disposición de los elementos, algunos de éstos se repiten y no intervienen necesariamente todos».

Teorema 19.39

Si X tiene n elementos, el *número de combinaciones con repetición de orden* k es $\binom{n+k-1}{k}$, esto es, $\frac{(n+k-1)!}{k!(n-1)!}$. $CR(n,k)$ —o, sinónimamente, $CR_{n,k}$, CR_k^n, ${}_nCR_k$, ${}^nCR_k$ o CR_n^k, o simplemente $\left(\!\binom{n}{k}\!\right)$— designa dicho número.

Observación 19.2.28.— $CR(n,k) = C_{n+k-1,k}$, esto es, $\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}$. Notemos que, en particular, $CR(n,0) = C_{n+0-1,0} = \frac{(n-1)!}{0!\cdot(n-1)!} = 1$.

Observación 19.2.29.— En lenguaje de multiconjuntos, $CR(n,k)$ es el número de multiconjuntos de cardinalidad k formados por elementos de un conjunto de cardinal n.

Ejemplo 649 (PRen7)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir tres tareas indistinguibles entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si cualquiera de éstos puede recibir cualquier número de tareas?

[SEP 12.5.2022:7], [EFEC 29.1.2025:10] (tipo test), [SEL 11:1a].

Resolución.— El computador central debe repartir tres tareas indistinguibles entre siete computadores distintos, sin ninguna restricción. En esta situación, cada reparto hecho por c_0 está representado por un submulticonjunto del conjunto de computadores auxiliares $C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7\}$. Por ejemplo, el reparto de dos tareas al computador c_3, una tarea al computador c_7 y ninguna tarea al resto de computadores, puede representarse por la combinación con repetición $\{\{c_3, c_3, c_7\}\}$, esto es, por dicho submulticonjunto de C.

Concluimos que el número de formas en las que c_0 puede repartir tres tareas idénticas entre siete computadores sin ninguna restricción es el número de combinaciones con repetición $CR(7,3) = C(7+3-1,3) = (7+3-1)!/(3!\cdot(7-1)!) = 84$. ■

Observación 19.2.30.— *Cfr. infra* § 19.2.10 (pág. 1182 de esta edición) y los ejemplos 650 y 682 (págs. 1181 y 1220 de esta edición) para estudiar otras vías de resolución.

§ 19.2.8 Definición funcional de combinación con repetición

Pudiésemos haber definido funcionalmente una combinación con repetición como una aplicación, en la siguiente forma.

Definición 19.22.— Si A es el conjunto subyacente del multiconjunto $[a_0, a_1, \dots, a_{n-1}]_{k,k,\dots,k}$, esto es, $\{\{a_0, \overset{k}{\dots}, a_0, a_1, \overset{k}{\dots}, a_1, \dots, a_{n-1}, \overset{k}{\dots}, a_{n-1}\}\}$, una combinación con repetición de orden k de elementos de A es una aplicación de A en $\{0, 1, \dots, k\}$ tal que a cada elemento a_i de $A = \{a_0, a_1, \dots, a_{n-1}\}$ le asocia el número de veces (entre 0 y k) que aparece repetido a_i en un submulticonjunto del multiconjunto, sujeta dicha aplicación a la condición de que la suma de tales números sea k. Observemos que tal aplicación define precisamente al submulticonjunto con esta característica.

Ejemplo 650 (PRen7bis)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir tres tareas indistinguibles entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si cualquiera de éstos puede recibir cualquier número de tareas?

[SEP 12.5.2022:7], [EFEC 29.1.2025:10] (tipo test), [SEL 11:1a].

Resolución.— En la situación en estudio, cada reparto efectuado por el computador central c_0 está representado por una aplicación del conjunto de computadores auxiliares $C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7\}$ en $\{0, 1, 2, 3\}$ tal que a cada computador auxiliar le asocia el número de tareas que le corresponden sujeta a la condición de que la suma de tales números es 3. El ejemplo que pusimos nos sirve: el reparto de dos tareas al computador c_3, una tarea al computador c_7 y ninguna tarea al resto de computadores auxiliares es tal que $0+0+2+0+0+0+1 = 3$, por lo que puede representarse por la combinación con repetición $\{\{c_3, c_3, c_7\}\}$, esto es, por dicho submulticonjunto del multiconjunto $\{\{c_1, c_1, c_1, c_2, c_2, c_2, \dots, c_7, c_7, c_7\}\}$. ■

§ 19.2.9 Definición relacional de combinación y combinación con repetición

Pudiésemos haber definido alternativamente los conceptos de combinación y combinación con repetición como clases de equivalencia, en la siguiente forma.

Definición 19.23.—

0. En la clase de todas las aplicaciones de $\{0, 1, \dots, k-1\}$ en un conjunto X no vacío, definimos la relación fRg si, y sólo si, $\operatorname{im} f = \operatorname{im} g$, que resulta ser de equivalencia, por lo que diremos que f y g son *aplicaciones equivalentes* según R;

1. una *combinación* de k elementos de un conjunto no vacío X es una clase de equivalencia de dicha relación R cuando se trate de aplicaciones inyectivas;

2. una *combinación con repetición* de k elementos de un conjunto no vacío X es una clase de equivalencia de dicha relación R cuando se trate de aplicaciones cualesquiera.

Y, por ejemplo, tenemos este teorema.

Teorema 19.40
Siendo R la relación anterior y X un conjunto con n elementos, el *número de combinaciones y de combinaciones con repetición* es el cardinal del conjunto cociente ${}^{X}/_{R}$ en cada caso.

§ 19.2.10 La ecuación diofántica $x_1 + x_2 + \ldots + x_n = k$ (Parte I)

Número de soluciones no negativas

En el ejemplo 649 (PRen7) (pág. 1180 de esta edición), también es posible representar cada reparto por una solución entera no negativa de la ecuación diofántica $x_1+x_2+\ldots+x_7 = 3$ donde x_i designa el número de tareas que recibe el computador auxiliar c_i, por lo que todo consiste en calcular *el número de soluciones enteras no negativas* ($x_i \geq 0$) de dicha ecuación (esto es consistente con el hecho de que como las tareas son indistinguibles, sólo importa el número de tareas que ha recibido cada computador auxiliar); dicho número, $CR(7, 3)$, es el número de formas de repartir las tareas.

Establecido el orden de interpretación $c_1c_2c_3c_4c_5c_6c_7$, las codificaciones cuaternarias 0020001, 1001010 y 0000300 son ejemplos de soluciones (corresponden a los submulticonjuntos $\{\{c_3, c_3, c_7\}\}$, $\{\{c_1, c_4, c_6\}\}$ y $\{\{c_5, c_5, c_5\}\}$ del multiconjunto $\{\{c_1, \overset{3}{\ldots}, c_1, c_2, \overset{3}{\ldots}, c_2, \ldots, c_7, \overset{3}{\ldots}, c_7\}\}$, respectivamente).

Teorema 19.41
El número de soluciones enteras no negativas de la ecuación diofántica $x_1 + x_2 + \ldots + x_n = k$ es $CR(n, k)$.

Observación 19.2.31.— Si $x_1 + x_2 + \ldots + x_n = 0$, la única solución no negativa es $(0, 0, \ldots, 0)$, en otras palabras, $CR(n, 0) = 0$, algo que ya sabíamos.

Observación 19.2.32.— Otra interpretación es una selección donde hay n tipos de objetos y la variable x_i representa el número de objetos que se seleccionan del tipo de objeto i.

Ejemplo 651 (PRen8)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir siete tareas, tres indistinguibles y cuatro distinguibles de esas tres y distinguibles también entre sí, entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si alguno de éstos puede no recibir ninguna tarea?

Resolución.— Nuestra estrategia de resolución comienza por calcular el número de repartos posibles de las cuatro tareas distinguibles —y, por ahora, como poder quedar, quedarán seguro computadores auxiliares sin recibir tarea—, para después determinar el número de repartos de las tareas indistinguibles y finalmente agregarlos mediante el principio de la multiplicación.

0.°, *Formalización del principio de la multiplicación:del suceso y las fases*.

El suceso

$S \leftrightharpoons$ se reparten siete tareas, tres indistinguibles y cuatro distinguibles a esas tres y distinguibles también entre sí, entre siete computadores auxiliares, pudiendo algunos de éstos no recibir ninguna tarea,

sucede en las dos fases sucesivas e independientes consecutivamente,

fase 0 $\leftrightharpoons$ se reparten cuatro tareas distinguibles entre siete computadores auxiliares, pudiendo algunos de éstos no recibir ninguna tarea,

fase 1 $\leftrightharpoons$ se reparten tres tareas indistinguibles entre siete computadores auxiliares, pudiendo algunos de éstos no recibir ninguna tarea.

1.°, *De las formas de realizar las fases*.

a. *Resolución de la fase* 0.

Decir «alguno de éstos puede no recibir ninguna tarea» no aporta información alguna, es como no decir nada.

Como cada computador auxiliar puede recibir más de una tarea, cada reparto de las cuatro tareas distinguibles corresponde a una aplicación cualquiera —sin ninguna condición— del conjunto de tareas $\{t_0, t_1, t_2, t_3\}$ en el conjunto no vacío C de computadores auxiliares; así, diremos que cada reparto de las cuatro tareas distinguibles es una variación con repetición de cuatro elementos de C, esto es, el número de posibles repartos de las cuatro tareas distinguibles es el número de variaciones con repetición, por lo tanto, existen —*cfr. supra* ejemplo 629 (pág. 1157 de esta edición)—

$$\begin{aligned} VR(7,4) &= 7^4 \\ &= 7 \cdot 7 \cdot 7 \cdot 7 \\ &= 2\,401 \end{aligned}$$

formas posibles de repartir las cuatro tareas distinguibles.

b. *Resolución de la fase* 1.

Ahora, pensemos en las tres tareas indistinguibles. Existen tantas formas de repartirlas como soluciones enteras no negativas tiene la ecuación $x_1 + x_2 + \cdots + x_7 = 3$ (x_i representa

el número de tareas que recibe el computador c_i), que son un total de $CR(7,3) = 84$ —*cfr. supra* teorema 19.41 (pág. 1182 de esta edición)—.

2.°, *Aplicación del principio de la multiplicación.*

Entonces, el suceso S se ha resuelto en dos fases sucesivas, independientes consecutivamente, por lo que por el principio de la multiplicación, el número de formas de repartir las tareas es

$$\begin{aligned} VR(7,4) \cdot CR(7,3) &= 2401 \cdot 84 \\ &= 201\,684. \end{aligned}$$

Solución.— De 201 684 formas. ■

Número de soluciones positivas

Ejemplo 652 (PRen9)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir diez tareas indistinguibles entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, de manera que cada uno de éstos reciba como mínimo una tarea?

[EFO 1.6.2017:5b], [EFO 20.5.2022:7b] (4 tareas, 3 computadores auxiliares, 3 formas), [SEL 11:1b]. *Cfr.* Franco, Espinel y Almeida [214]: ejercicio 7.1 (págs. 138–139).

Resolución.— Exploremos dos vías.

Vía 0.

Como las tareas son indistinguibles, sólo importa el número de tareas que ha recibido cada computador auxiliar, esto es, se trata de calcular *el número de soluciones enteras positivas* (x_i representa el número de tareas que recibe el computador c_i) ($x_i \geq 1$, porque cada computador auxiliar debe recibir al menos una tarea) de la ecuación

$$x_1 + x_2 + \ldots + x_7 = 10. \qquad (19.0)$$

Por el teorema 19.41 (pág. 1182 de esta edición), sabemos que el número de soluciones no negativas, esto es, si $x_i \geq 0$, de esta ecuación viene dado por $CR(7,10)$. Sin embargo, buscamos soluciones positivas, esto es, si $x_i \geq 1$. Una vía de resolución consiste en transformar la ecuación 19.0 en una ecuación sujeta a la condición de no negatividad de sus variables (que es la que sabemos por dicho teorema que corresponde a las combinaciones con repetición).

Para conseguirlo, hacemos el cambio de variable $y_i = x_i - 1$, de lo que se sigue que $x_i \geq 1 \leftrightarrow x_i - 1 \geq 1 - 1 \leftrightarrow y_i \geq 0$. Ahora, si restamos 1 a cada incógnita en la ecuación (19.0), entonces

$(x_1 - 1) + (x_2 - 1) + \cdots + (x_7 - 1) = 10 - (1+1+1+1+1+1+1)$ y, así, la ecuación (19.0) se ha transformado en $y_1 + y_2 + \cdots + y_7 = 10 - 7$, con $y_i \geq 0$, que como sabemos por el teorema 19.41 (pág. 1182 de esta edición), su número de soluciones enteras no negativas es $CR(7, 10-7) = 84$, siendo éste el número de formas buscado de repartir las tareas. □

Vía 1.

Asignamos una tarea cada computador auxiliar, esto es, hacemos que se satisfaga el requisito impuesto (que cada uno reciba como mínimo una tarea). Ya hemos repartido siete tareas. Para asignar las $10-7$ tareas restantes no existe ningún requisito, por lo que es posible asignarlas de $CR(7, 10-7)$ formas —*vid. supra* ejemplo 649 (pág. 1180 de esta edición) (PRen7)—. En otras palabras, hemos reducido el problema PRen9 al PRen7. ■

Solución.— De 84 formas.

Observación 19.2.33.— $CR(7, 10-7) = CR(7,3) = C(7+3-1, 3) = C(9,3) = C(9,6) = C(10-1, 7-1)$. El siguiente teorema aborda el caso general.

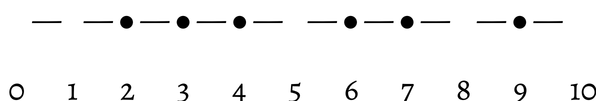
Teorema 19.42

El número de soluciones enteras positivas de la ecuación diofántica $x_1 + x_2 + \ldots + x_n = k$, $n \leq k$, es $C(k-1, n-1)$.

[SEL 9:5].

Demostración.— Demostrémoslo codificando gráficamente la información. En efecto, sucede tal como enuncia este teorema, ya que la cuestión equivale a calcular cuántas formas existen de situar $n-1$ marcas sobre las $k-1$ divisiones de un segmento de longitud k.

Por ejemplo, una forma de posicionar seis marcas (las marcas son los •) sobre las nueve divisiones de un segmento de longitud diez es:



que corresponde a la solución positiva $\langle x_1, x_2, x_3, x_4, x_5, x_6, x_7 \rangle = \langle 2, 1, 1, 2, 1, 2, 1 \rangle$ de $x_1 + x_2 + \ldots + x_7 = 10$ —dos unidades hasta la primera marca (situada sobre la segunda división del segmento), después una unidad hasta la segunda marca (situada sobre la tercera división), después una unidad hasta la tercera marca (situada sobre la cuarta división), después dos unidades hasta la cuarta marca (situada sobre la sexta división), después una unidad hasta la quinta marca (situada sobre la séptima división) y finalmente dos unidades hasta la sexta marca (situada sobre la novena división)—. Cada posicionamiento es un subconjunto de seis elementos del conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ (en este ejemplo,

el subconjunto $\{2,3,4,6,7,9\}$), esto es, una combinación de seis elementos de dicho conjunto[21]. El número de posicionamientos es el número de combinaciones de seis elementos de dicho conjunto, esto es, $C(9,6) = 84$. Observemos que $\{2,3,4,6,7,9\}$ es una *codificación conjuntista* de la solución $\langle 2,1,1,2,1,2,1\rangle$, 234679 y 734296 son *codificaciones decimales* y la palabra 011101101 es una *codificación binaria* (0 indica posición no marcada y 1 marcada).

Observemos que el número de soluciones positivas de $x_1+x_2+\ldots+x_7 = 10$ es $C(10-1,7-1)$. Análogamente, el número de soluciones positivas de $x_1+x_2+\ldots+x_n = k$ es $C(k-1,n-1)$. ■

Número de soluciones no negativas acotadas inferiormente

Ejemplo 653 (PRen10)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir k tareas indistinguibles entre n computadores auxiliares, $c_1, c_2, c_3, \ldots, c_n$, de manera que cada uno de éstos reciba como mínimo m tareas? Suponemos que $m \cdot n \leq k$.

Resolución.— Es admisible enunciar alternativamente esta cuestión así: calculemos el número de soluciones no negativas de $x_1+x_2+\cdots+x_n = k$, si $\forall i \in \{1,2,\ldots,n\}, x_i \geq m$, con $m \cdot n \leq k$.

Para su resolución, hacemos el cambio de variable $y_i = x_i - m$, de lo que se sigue que $x_i \geq m \leftrightarrow x_i - m \geq m - m \leftrightarrow y_i \geq 0$.

(Lo hacemos porque nos interesan las variables no negativas, ya que sabemos que entonces cada solución no negativa es una combinación con repetición).

Ahora, restando m a cada incógnita en la ecuación original, $(x_1-m)+(x_2-m)+\cdots+(x_n-m) = k-m\cdot n$, dicha ecuación queda $y_1+y_2+\cdots+y_n = k-m\cdot n$, con $y_i \geq 0$, cuyo número de soluciones enteras no negativas es $CR(n, k-m\cdot n)$ —*cfr. supra* teorema 19.41 (pág. 1182 de esta edición)—. ■

Teorema 19.43
El número de soluciones no negativas de $x_1+x_2+\cdots+x_n = k$, si $\forall i \in \{1,2,\ldots,n\}, x_i \geq m$, con $m\cdot n \leq k$, es $CR(n, k-m\cdot n)$.

[21] No marcamos 0 porque buscamos soluciones positivas y no es necesario que marquemos 10 porque la última componente de la solución viene determinada por la longitud desde la última marca hasta 10.

Número de soluciones no negativas con una componente fija acotada superiormente

Ejemplo 654 (PRen11)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir k tareas indistinguibles entre n computadores auxiliares, $c_1, c_2, c_3, \ldots, c_n$, de manera que exactamente uno de ellos reciba como mucho m tareas? Suponemos que $m < k$.

Resolución.— Es admisible enunciar alternativamente esta cuestión así: calculemos el número de soluciones no negativas de $x_1 + x_2 + \cdots + x_n = k$, si $\forall i \in \{1, 2, \ldots, n\}, 0 \leq x_1 \leq m$, con $m < k$.

Intuitivamente, el resultado buscado es el número de soluciones enteras no negativas menos el número de ellas que satisfacen $x_1 \geq m + 1$.

Esto es, por un lado, el número de soluciones enteras no negativas de $x_1 + x_2 + \cdots + x_n = k$ es $CR(n, k)$; por otro, calculemos el número de soluciones enteras no negativas de $x_1 + x_2 + \cdots + x_n = k$que satisfacen $x_1 \geq m + 1$, algo que es posible hacer de manera parecida a como hemos resuelto el ejemplo anterior.

Hacemos el cambio de variable $y_1 = x_1 - (m + 1)$, entonces $x_1 \geq m + 1 \leftrightarrow x_1 - (m + 1) \geq (m + 1) - (m + 1) \leftrightarrow y_1 \geq 0$. Ahora, restando $m + 1$ a la primera incógnita en la ecuación original, $(x_1 - (m + 1)) + x_2 + \cdots + x_n = k - (m + 1)$ y, así, la ecuación original se ha transformado en $y_1 + x_2 + \cdots + x_n = k - (m + 1)$, con $y_1 \geq 0, x_2 \geq 0, \ldots, x_n \geq 0$, por lo que el número de sus soluciones enteras no negativas es $CR(n, k - (m + 1))$ —*cfr. supra* teorema 19.41 (pág. 1182 de esta edición)—.

Para hallar el resultado final que buscamos, vamos a utilizar el principio del complementario. Siendo $B = \{x : x \text{ es una solución entera no negativa de } x_1 + x_2 + \cdots + x_n = k\}$ y $A = \{x : x \text{ es una solución entera no negativa de } x_1 + x_2 + \cdots + x_n = k \text{ que satisface } x_1 \leq m\}$, tenemos que $B \setminus A = \{x : x \text{ es una solución entera no negativa de } x_1 + x_2 + \cdots + x_n = k \text{ tal que } x_1 \geq m + 1\}$, entonces el número de soluciones buscado (el número de soluciones no negativas menos el número de ellas que satisfacen $x_1 \geq m + 1$) es $|A| = |B| - |B \setminus A| = CR(n, k) - CR(n, k - (m + 1))$. ■

Teorema 19.44

El número de soluciones no negativas de $x_1 + x_2 + \cdots + x_n = k$, si $\forall i \in \{1, 2, \ldots, n\}, 0 \leq x_1 \leq m$, con $m < k$, es $CR(n, k) - CR(n, k - (m + 1))$, esto es, $C(n + k - 1, k) - C(n + k - m - 2, k - m - 1)$.

§ 19.2.11 Número de permutaciones circulares

Ya hemos estudiado las permutaciones circulares *cfr. supra* definición 17.40 (pág. 873 de esta edición). Ahora nos interesa su número.

Ejemplo 655

¿De cuántas formas no equivalentes pueden sentarse cuatro personas alrededor de una mesa redonda en cuatro asientos? (Consideramos dos formas equivalentes precisamente si cada persona tiene las mismas personas sentadas a derecha e izquierda).

Resolución.— Hay cuatro asientos, digamos A, B, C y D, luego hay cuatro personas disponibles para el asiento A, tres personas para el B, dos para el C y una persona para el asiento D; un total, por el principio de la multiplicación, de $4 \cdot 3 \cdot 2 \cdot 1 = 24$, es decir, el suceso «sentarse cuatro personas en cuatro asientos» ocurre de $n = 24$ formas —esto es justo el comienzo del enunciado del principio de la división—.

Nombrando ahora las personas R, S, T, U, y fijándonos, por ejemplo, en la forma de sentarse (R, S, T, U), existen cuatro disposiciones (formas de sentarse) equivalentes (dos formas son equivalentes precisamente si cada persona tiene las mismas personas sentadas a derecha e izquierda): (R, S, T, U), (U, R, S, T), (T, U, R, S) y (S, T, U, R).

Este hecho de haber 4 formas de sentarse equivalentes para una dada, sucede para cualquier forma de sentarse. Es decir, cualquier forma distinta de sentarse sucede de $d = 4$ de las $n = 24$ formas.

Por tanto, por el principio de la división, hay $24/4 = 6$ formas distintas en las que cuatro personas pueden sentarse alrededor de una mesa redonda en cuatro asientos. ■

Observación 19.2.34.— Pues sí, cada una de las formas distintas (no equivalentes) de sentarse (R, S, T, U), (R, S, U, T), (R, T, S, U), (R, T, U, S), (R, U, S, T) y (R, U, T, S) sucede de $d = 4$ de las $n = 24$ formas:

$$\begin{aligned}
D_{RSTU} &= \{(R, S, T, U), (U, R, S, T), (T, U, R, S), (S, T, U, R)\},\\
D_{RSUT} &= \{(R, S, U, T), (T, R, S, U), (U, T, R, S), (S, U, T, R)\},\\
D_{RTSU} &= \{(R, T, S, U), (U, R, T, S), (S, U, R, T), (T, S, U, R)\},\\
D_{RTUS} &= \{(R, T, U, S), (S, R, T, U), (U, S, R, T), (T, U, S, R)\},\\
D_{RUST} &= \{(R, U, S, T), (T, R, U, S), (S, T, R, U), (U, S, T, R)\},\\
D_{RUTS} &= \{(R, U, T, S), (S, R, U, T), (T, S, R, U), (U, T, S, R)\}.
\end{aligned}$$

Éstos son los seis conjuntos disjuntos de formas distintas. En efecto, somos capaces de demostrar que $i \neq j \to D_i \cap D_j = \emptyset$ (formas distintas —no equivalentes— no suceden de la misma forma).

Observación 19.2.35.— En la formulación del principio en términos de conjuntos, $X = D_{RSTU} \cup D_{RSUT} \cup D_{RTSU} \cup D_{RTUS} \cup D_{RUST} \cup D_{RUTS}$, que como dijimos son conjuntos disjuntos dos a dos.

Observación 19.2.36.— Cada una de estas seis formas distintas, (R, S, T, U), (R, S, U, T), (R, T, S, U), (R, T, U, S), (R, U, S, T) y (R, U, T, S), se conoce como una *permutación circular* de las cuatro «entidades» R, S, T y U. En general, el *número de permutaciones circulares* de n entidades es $(n-1)!$ (en este ejemplo, $(4-1)! = 6$). No hay una notación estándar para el número de permutaciones circulares de n entidades, utilizaremos $\overset{\circ}{P}(n)$.

Ejemplo 656

¿Y si las personas R y S quieren sentarse juntas?

Resolución.— Tenemos que considerar dos posibilidades, a saber, que R y S se sienten así (R, S) o así (S, R); como R y S quieren sentarse juntas, en cualquiera de estos dos casos es como si hubiera un total de tres personas (esto es, $n = 3 \cdot 2 \cdot 1 = 6$, $d = 3$, y por el principio de la división, hay $6/3$ formas distintas), por lo que el resultado final, como hay dos casos, (R, S) y (S, R), es $2 \cdot (6/3) = 4$ formas. ■

Observación 19.2.37.— Utilizando permutaciones circulares, tenemos $2 \cdot \overset{\circ}{P}(3) = 2 \cdot (3-1)! = 4$.

Actividad 19.14

Cierto es que $2 \cdot 6/3 = 6/3 + 6/3$. ¿Pudiésemos interpretar esta suma como un resultado del principio de la adición?

Ejemplo 657

¿Y si las personas R y S quieren sentarse separadas?

Resolución.— Por el principio del complementario, siendo $B = \{x : x$ es una forma distinta de sentarse cuatro personas en cuatro sillas en una mesa redonda$\}$ y $A = \{x : x$ es una forma distinta de sentarse cuatro personas en cuatro sillas en una mesa redonda si dos determinadas quieren sentarse separadas$\}$, entonces, como $|B \backslash A|$ es el número de formas en que pueden sentarse juntas (*cfr.* ejemplo anterior), $|A| = |B| - |B \setminus A| = 6 - 4 = 2$ formas.

En otras palabras, $\overset{\circ}{P}(4) - 2 \cdot \overset{\circ}{P}(3) = (4-1)! - 2 \cdot (3-1)! = 6 - 4 = 2.$ ■

Actividad 19.15

¿De cuántas formas se pueden organizar las cuentas de una pulsera de siete cuentas?

Matemagia: *el mejor truco de cartas*

Un ejemplo de matemagia que combina para su solución el principio de los cajones, relaciones de orden, aritmética modular y permutaciones; lo podemos conocer en *DivulgaMat*[22]: https://www.divulgamat.net/index.php?option=com_content&view=article&id=14733&directory=67.

§ 19.3 Modelización de problemas de recuento simple

No es lo mismo. Ni siquiera se le parece. O sí. Sea como sea, el *diseño de patrones* (*cfr. v. gr.* Talla [215]) comparte similaridades con la modelización. ¿Por qué resolver un problema dos veces? Pensar en un modelo, en una reminiscencia a la que ajustar el nuevo problema, en eso consiste este camino.

En combinatoria se distinguen cinco tipos de problemas básicos: *de existencia*, *de enumeración*, *de recuento*, *de clasificación* y *de optimización*. En esta breve introducción tratamos sólo cuatro modelizaciones de problemas de recuento simple (*cfr.* Dubois [216]).

§ 19.3.0 Modelización I: selección o muestreo simple

Se trata de las formas simples en que se pueden seleccionar —o extraer una muestra de— k objetos de un total de n objetos distinguibles $o_0, o_1, \ldots, o_{n-1}$ y el número total de cada una de tales formas simples.

[22] *Vid*. http://www.divulgamat.net/.

Teorema 19.45 (Modelización I: esquema de interpretaciones)

Cuadro n.º 0
Los cuatro tipos de selecciones simples
de k objetos de un total de n objetos distinguibles

Selección (muestra)	Reposición de objetos	N.º de selecciones
Ordenada	Sin reemplazamiento	$V(n,k)$
(el orden de los objetos importa	Con reemplazamiento	$VR(n,k)$
para distinguir dos muestras)		
No ordenada	Sin reemplazamiento	$C(n,k)$
	Con reemplazamiento	$CR(n,k)$

Como sabemos, el caso particular $V(n,n)$ lo conocemos como $P(n)$ y corresponde al número de muestras ordenadas sin reemplazamiento de n objetos de un conjunto de n objetos distinguibles.

Observación 19.3.0.— ¿Por qué $CR(n,k)$? Representemos los n objetos distinguibles como n cartas numeradas de 1 a n. Nos interesa el número de manos de k cartas que pueden formarse a partir del mazo de n cartas, permitiendo la repetición. Para ello, añadimos $k-1$ cartas extra («comodines»), numeradas de $n+1$ a $n+k-1$ y que portan las instrucciones:

$n+1$: repetir la carta de numeración más baja;

$n+2$: repetir la 2.ª carta de numeración más baja;

$\vdots$

$n+k-1$: repetir la $(k-1)$-ésima carta de numeración más baja.

Entonces, existe una biyección entre las manos de k cartas sin repetición de este mazo agrandado de $k+r-1$ cartas y las manos de k cartas con repetición del mazo original de n cartas[23].

Ejemplo 658

En una fila de 7 sillas, ¿de cuántas formas se pueden sentar 3 personas?

[SEL 9:6].

[23] Esta respuesta es de Solomon Wolf Golomb y aparece en «Combinatorial Communication: A New Interpretation of a Basic Combinatorial Formula», publicado en JPL [Jet Propulsion Laboratory] *Space Programs Summary* 37-42, Vol. IV (Supporting Research and Advanced Development —Unclassified—), págs. 197-198, California Institute of Technology, Pasadena, California (31 de diciembre de 1966) (https://ntrs.nasa.gov/citations/19670009018).

Resolución.— Pudiésemos razonar, bien por definición, bien por alguna de las cuatro modelizaciones.

Por ejemplo, por definición y por la primera modelización.

Vía 0.
(Por definición).

Cada sentada es una aplicación inyectiva de $\{0, 1, 2\}$ en el conjunto de las sillas $S = \{s_0, \ldots, s_6\}$, esto es, una variación de $k = 3$ elementos del conjunto no vacío S de 7 elementos —es aplicación (función total) porque es función, ya que cualquier persona, de sentarse, lo haría en una sola silla y concretamente es una función total porque las tres personas han de sentarse; es inyectiva porque no es posible que más de una persona se sienten simultáneamente en una misma silla—. El número de dichas variaciones es $V(7, 3) = 7 \cdot 6 \cdot 5 = 210$, siendo éste el número de sentadas. □

Vía 1.
(Por la modelización I).

Cada sentada es una selección simple ordenada de $k = 3$ objetos de un total de $n = 7$ objetos distinguibles (las sillas). Es ordenada porque la elección de una silla se hace efectiva mediante la asignación de una persona que se sienta en ella, siendo entonces como si la persona «etiquetase» la silla, por lo que, si por ejemplo, las personas son P_0, P_1 y P_2, en realidad las sillas elegidas, vemos cómo el orden importa, pues no es lo mismo la sentada $\langle P_0, P_1, P_2\rangle$ que la sentada $\langle P_1, P_0, P_2\rangle$. En definitiva, el número total de sentadas es el número total de variaciones, $V(7, 3) = 7 \cdot 6 \cdot 5 = 210$. ■

Ejemplo 659

¿Cuántas palabras decimales diferentes de longitud diez hay que contienen los primeros cinco dígitos, $0, 1, 2, 3, 4$ (llamémoslas letras de tipo I), y los segundos cinco dígitos $5, 6, 7, 8, 9$ (llamémoslas letras de tipo II), y tales que las letras de tipo II no figuren juntas?

Resolución.— Apliquemos el principio de la multiplicación.

0.°, *Formalización del principio de la multiplicación: del suceso y sus fases.*

Para poder aplicar el principio de la multiplicación debemos definir un suceso descompuesto en fases sucesivas e independientes consecutivamente.

Sea el suceso

$S \leftrightharpoons$ la «construcción» de una palabra decimal de longitud diez tal que las letras de tipo II no figuren juntas,

que ocurre en cuatro fases sucesivas e independientes consecutivamente:

$S_0 \leftrightharpoons$ la construcción de una palabra de longitud cinco tal que todas sus letras son de tipo I,

$S_1 \leftrightharpoons$ la acción de dejar un hueco entre cada dos de estas letras y al principio y al final,

$$\square\, 0 \,\square\, 1 \,\square\, 2 \,\square\, 3 \,\square\, 4 \,\square$$

(pues entonces podremos colocar las cinco letras de tipo II en estos huecos y así satisfacer la restricción impuesta, a saber, que no pueden figurar juntas dos letras de tipo II).

$S_2 \leftrightharpoons$ la selección de cinco de los seis «huecos» entre las letras de la palabra anterior,

$S_3 \leftrightharpoons$ la reordenación de las cinco letras de tipo II.

Cuatro fases que son sucesivas e independientes consecutivamente.

1.°, *De las formas de realizar las fases*.

- Fase S_0: existen 120 formas distintas de realizarla, ya que existen $V(5,5) = P(5) = 5! = 120$ palabras de longitud cinco tales que todas sus letras son de tipo I (cada forma es una selección ordenada sin reemplazamiento de cinco objetos [las cinco letras de tipo I] de un total de cinco objetos distinguibles [las cinco letras de tipo I]).
- Fase S_1: existe sólo una forma de realizarla.
- Fase S_2: existen seis formas distintas de realizarla, ya que elegimos cinco de los seis huecos para colocar las cinco letras de tipo II, lo que es posible hacer de $C(6,5)$ formas (cada forma es una selección no ordenada sin reemplazamiento de cinco objetos [cinco huecos] de un total de seis objetos distinguibles [los seis huecos]).
- Fase S_3: existen 120 formas de realizarla, pues es posible ordenar las cinco letras de tipo II de $V(5,5) = P(5) = 5! = 120$ formas diferentes (cada forma es una selección ordenada sin reemplazamiento de cinco objetos [las cinco letras de tipo II] de un total de cinco objetos distinguibles [las cinco letras de tipo II]).

2.°, *Aplicación del principio de la multiplicación*.

Nuestro interés es averiguar el número de formas en que sucede el suceso S. Como hemos dicho ya, S ocurre en cuatro fases sucesivas e independientes consecutivamente, así que es admisible aplicar el principio de la multiplicación. Notando por $\#X$ el número de formas en que sucede un suceso X y también el número de formas en que se realiza una fase X, existen

$$\begin{aligned} \#S &= \#S_0 \cdot \#S_1 \cdot \#S_2 \cdot \#S_3 \\ &= 5! \cdot 1 \cdot \binom{6}{5} \cdot 5! \\ &= 86\,400 \end{aligned}$$

formas de que suceda el suceso S.

Solución.— Existen 86 400 diferentes palabras decimales con estas características. ■

Ejemplo 660

En las condiciones del ejemplo 659 (pág. 1192 de esta edición), ¿cuántas palabras decimales diferentes de longitud diez hay que contienen las letras de tipo I y las letras de tipo II y son tales que en cualquier subpalabra de longitud dos, siempre hay una de las letras de tipo I y una de las letras de tipo II?

[Cubit 140].

Resolución.— Sea ahora el suceso

$S \leftrightharpoons$ la construcción de una palabra decimal de longitud diez tal que en cualquier subpalabra de longitud dos hay una de las letras de tipo I y una de las de tipo II.

Vía 0.

En la fase S_2 —*cfr. supra* ejemplo 659 (pág. 1192 de esta edición), la elección de cinco de los seis huecos puede hacerse de dos formas, a saber, a la izquierda de las letras de tipo I, por ejemplo,

$$5\,0\,6\,1\,7\,2\,8\,3\,9\,4\,\square,$$

o bien, a la derecha de las letras de tipo I, por ejemplo,

$$\square\,0\,5\,1\,6\,2\,7\,3\,8\,4\,9,$$

(existen dos formas de realizarla, ya que elegimos no rellenar uno de los dos huecos exteriores sin ninguna restricción, lo que es posible hacer de $V(5,1) = 2$ formas diferentes —cada forma es una selección ordenada sin reemplazamiento de un objeto [uno de los dos huecos exteriores] de un total de dos objetos distinguibles [los dos huecos exteriores]—), en definitiva, $\#S_2 = 2$, por lo que, por el principio de la multiplicación, existen $\#S = \#S_0 \cdot \#S_1 \cdot \#S_2 \cdot \#S_3 = 5! \cdot 1 \cdot 2 \cdot 5! = 28\,800$ formas de que suceda el suceso S. □

Vía 1.

Alternativamente, las fases S_2 y S_3 pudiesen ser:

$S_2 \leftrightharpoons$ la colocación de cuatro de las cinco letras de tipo II en los cuatro huecos interiores (huecos entre las letras 0 y 4),

$S_3 \leftrightharpoons$ la colocación de una letra de tipo II en los huecos exteriores.

Tenemos que:

- Fase S_2: existen 120 formas distintas de realizarla, ya que elegimos cuatro de las cinco letras de tipo II sin ninguna restricción, lo que es posible hacer de $V(5,4)$ formas (cada forma es una selección ordenada sin reemplazamiento de cuatro objetos [cuatro letras] de un total de cinco objetos distinguibles [las cinco letras de tipo II]).

- Fase S_3: existen dos formas de realizarla, ya que elegimos rellenar uno de los dos huecos exteriores sin ninguna restricción, lo que es posible hacer de $V(2,1) = 2$ formas diferentes (cada forma es una selección ordenada sin reemplazamiento de un objeto [uno de los dos huecos exteriores] de un total de dos objetos distinguibles [los dos huecos exteriores]).

Por el principio de la multiplicación, existen $\#S = \#S_0 \cdot \#S_1 \cdot \#S_2 \cdot \#S_3 = 5! \cdot 1 \cdot 120 \cdot 2 = 28\,800$ formas de que suceda el suceso S. □

Vía 2.[24]

Vemos S como unión de dos sucesos que no pueden suceder a la vez:

$S_0 \leftrightharpoons$ la construcción de una palabra decimal de longitud diez tal que en cualquier subpalabra de longitud dos hay una de las letras de tipo I y una de las de tipo II y tal que las posiciones de lugar impar están ocupadas por las cinco letras de tipo I.

$S_1 \leftrightharpoons$ la construcción de una palabra decimal de longitud diez tal que en cualquier subpalabra de longitud dos hay una de las letras de tipo I y una de las de tipo II y tal que las posiciones de lugar impar están ocupadas por las cinco letras de tipo II.

Subyace, por tanto, el principio de la adición. Para poder aplicarlo debemos averiguar de cuántas formas suceden S_0 y S_1. El análisis para ambos es similar.

Formas en que sucede S_0.

$S_{00} \leftrightharpoons$ la construcción de una palabra de longitud cinco tal que todas sus letras son de tipo I,

$S_{01} \leftrightharpoons$ la acción de dejar un hueco entre cada dos de estas letras y al principio,

$$\square\, 0\, \square\, 1\, \square\, 2\, \square\, 3\, \square\, 4$$

$S_{02} \leftrightharpoons$ la selección ordenada sin reemplazamiento de las cinco letras de tipo II (destinadas a colocarse en esos cinco huecos).

Tres fases que son sucesivas e independientes consecutivamente. Con respecto a las formas de realizarlas, tenemos:

- Fase S_{00}: existen 120 formas distintas de realizarla [ya lo hemos discutido anteriormente].

- Fase S_{01}: existe sólo una forma de realizarla.

[24] A partir de una idea de Jorge Sánchez Gil (año académico 2024-2025).

- Fase S_{02}: existen 120 formas distintas de realizarla, ya que elegimos cinco de las cinco letras de tipo II sin ninguna restricción, lo que es posible hacer de $V(5,5)$ formas (cada forma es una selección ordenada sin reemplazamiento de cinco objetos [cinco letras] de un total de cinco objetos distinguibles [las cinco letras de tipo II]).

Por el principio de la multiplicación, existen $\#S_0 = \#S_{00} \cdot \#S_{01} \cdot \#S_{02} = 120 \cdot 1 \cdot 120 = 14\,400$ formas de que suceda el suceso S_0.

Formas en que sucede S_1.

$S_{10} \leftrightharpoons$ la construcción de una palabra de longitud cinco tal que todas sus letras son de tipo II,

$S_{11} \leftrightharpoons$ la acción de dejar un hueco entre cada dos de estas letras y al principio,

$$\square\, 5\, \square\, 6\, \square\, 7\, \square\, 8\, \square\, 9$$

$S_{12} \leftrightharpoons$ la selección ordenada sin reemplazamiento de las cinco letras de tipo I (destinadas a colocarse en esos cinco huecos).

Tres fases que son sucesivas e independientes consecutivamente. Con respecto a las formas de realizarlas, tenemos:

- Fase S_{10}: existen 120 formas distintas de realizarla [ya lo hemos discutido anteriormente].
- Fase S_{11}: existe sólo una forma de realizarla.
- Fase S_{12}: existen 120 formas distintas de realizarla, ya que elegimos cinco de las cinco letras de tipo I sin ninguna restricción, lo que es posible hacer de $V(5,5)$ formas (cada forma es una selección ordenada sin reemplazamiento de cinco objetos [cinco letras] de un total de cinco objetos distinguibles [las cinco letras de tipo I]).

Por el principio de la multiplicación, existen $\#S_1 = \#S_{10} \cdot \#S_{11} \cdot \#S_{12} = 120 \cdot 1 \cdot 120 = 14\,400$ formas de que suceda el suceso S_1.

Entonces, por el principio de la adición, tenemos que existen $\#S = \#S_0 + \#S_1 = 14\,400 + 14\,400 = 28\,800$ formas de que suceda el suceso S. ■

§ 19.3.1 Modelización II. Distribución, almacenamiento o colocación simple

Se trata de las formas simples en que es posible distribuir, almacenar o colocar k objetos en n recipientes (también se conocen como problemas de ocupación —de recipientes por objetos—). Representamos cada una de estas formas simples, esto es, cada distribución de k objetos en n recipientes, por una aplicación $f : O \longrightarrow R$, donde O es el conjunto o multiconjunto de objetos y R el conjunto o multiconjunto de recipientes.

Número de distribuciones

Al distribuir objetos en recipientes, debemos tener en cuenta:

A. El tipo de la aplicación $f : O \longrightarrow R$ representa la situación de los recipientes con respecto a los objetos —*cfr. infra* teorema 19.46 (pág. 1197 de esta edición)—).

Teorema 19.46 (Modelización II: estado de los recipientes y tipo de aplicación)

Cuadro n.º 1
Correspondencia entre la situación de los n recipientes
y el tipo de la aplicación, $f : O \longrightarrow R$, de los k objetos en los n recipientes

Situación de los n recipientes	Tipo de $f : O \longrightarrow R$
Puede haber algunos vacíos o con más de un objeto	Cualquiera
Ninguno contiene más de un objeto	Inyectiva ($k \leq n$)
Cada uno contiene al menos un objeto	Sobreyectiva ($k \geq n$)
Cada uno contiene exactamente un objeto	Biyectiva ($k = n$)

B. También hemos de considerar que tanto los objetos como los recipientes sean distinguibles o indistinguibles, diferenciándose, pues, cuatro posibilidades.

C. Además, consideramos la posibilidad de que los objetos estén ordenados (o no) en los recipientes.

De este modo, dado que hemos descompuesto la ocurrencia del suceso ser una distribución simple de k objetos en n recipientes en tres fases independientes consecutivamente, cuyos números de formas de realización son:

- $\#S_A = 4$, por ser cuatro los tipos de aplicación $f : O \longrightarrow R$ (cualquiera, inyectiva, sobreyectiva, biyectiva);
- $\#S_B = 4$, por ser cuatro las posibilidades de distinguibilidad/indistinguibilidad para objetos y recipientes;
- $\#S_C = 2$, por ser dos las posibilidades para los objetos dentro de los recipientes, ordenados o no,

entonces, por el principio de la multiplicación, tenemos un total de $4 \cdot 4 \cdot 2 = 32$ casos, pero como la distinción entre distribuciones ordenadas de objetos indistinguibles carece de sentido (imaginemos tratar de ordenar tres bolas rojas indistinguibles dentro de un mismo recipiente, sin más, sin nada externo, imposible), hay que excluir ocho casos, por lo que el número de tipos distintos de distribuciones simples es 24.

En definitiva, se trata de contar el número total de distribuciones en cada uno de los 24 tipos.

Distribuciones no ordenadas

El siguiente teorema muestra los 16 tipos de distribuciones simples no ordenadas y el número de distribuciones para cada tipo.

Como hemos dicho, por *distribución no ordenada* nos referimos a que no influye en el recuento el orden de los objetos dentro de los recipientes, esto es, que dos distribuciones no son distintas porque sean distintos tales órdenes.

Teorema 19.47 (Modelización II: esquema de interpretaciones: distrib. no ordenadas)

Cuadro n.º 2.a

Los 16 tipos de distribuciones simples no ordenadas de k objetos en n recipientes

Distribución	Objetos	Recipientes	Aplicación	N.º de distribuciones
No ordenada	Distinguibles	Distinguibles	Cualquiera	$VR(n,k)$
			Inyectiva	$V(n,k)$
			Sobreyectiva	$P(n)S(k,n)$
			Biyectiva	$P(n)$
		Indistinguibles	Cualquiera	$\Sigma(k,n)$
			Inyectiva	1
			Sobreyectiva	$S(k,n)$
			Biyectiva	1
	Indistinguibles	Distinguibles	Cualquiera	$CR(n,k)$
			Inyectiva	$C(n,k)$
			Sobreyectiva	$CR(n,k-n)$
			Biyectiva	1
		Indistinguibles	Cualquiera	$\Pi(k,n)$
			Inyectiva	1
			Sobreyectiva	$p(k,n)$
			Biyectiva	1

Ejemplo 661

¿Cuántos resultados son posibles al tirar k dados?

[Cubit 142].

Resolución.— Pensemos según la modelización II. Las puntuaciones de un dado hacen de recipientes, distinguibles, seis en total; los objetos, indistinguibles, son marcas, k en total. Esto es, cada

tirada de los k dados está representada por una distribución de k objetos indistinguibles (k marcas) en seis recipientes distinguibles. Por lo tanto, esta cuestión equivale a preguntarnos cuántas de tales distribuciones existen. Al ser los objetos indistinguibles, el orden de éstos en los recipientes no influye en el recuento de distribuciones; en otras palabras, se trata de una distribución no ordenada. Como puede haber recipientes con más de un objeto y puede haberlos vacíos, no hay restricciones para la aplicación subyacente $f : O \longrightarrow R$ del multiconjunto de objetos (las k marcas) en el conjunto de recipientes (las 6 puntuaciones). Por todo esto y lo establecido en el cuadro n.º 2a —teorema 19.47 (pág. 1198 de esta edición)—, el número de distribuciones es $CR(6, k)$.

Por ejemplo, con 12 dados, la tirada $\langle 1, 5, 3, 3, 6, 1, 2, 6, 4, 3, 2, 4\rangle$ es la distribución no ordenada $\{\checkmark \longmapsto 1, \checkmark \longmapsto 5, \checkmark \longmapsto 3, \checkmark \longmapsto 3, \checkmark \longmapsto 6, \checkmark \longmapsto 1, \checkmark \longmapsto 2, \checkmark \longmapsto 6, \checkmark \longmapsto 4, \checkmark \longmapsto 3, \checkmark \longmapsto 2, \checkmark \longmapsto 4\}$, gráficamente

1	2	3	4	5	6
✓ ✓	✓ ✓	✓ ✓ ✓	✓ ✓	✓	✓ ✓

—que, por cierto, pudiésemos codificar como esta palabra de seis letras en el sistema tridecimal (base 13) (son doce objetos): 223212—; así, existen $CR(6, 12) = \binom{6+12-1}{12} = 6188$ resultados posibles al tirar 12 dados.

Solución.— Existen $CR(6, k)$ resultados posibles. ■

Ejemplo 662

¿Cuántos números naturales de tres cifras son tales que sus cifras suman nueve?

[Cubit 143].

Resolución.— Para que el número sea de tres cifras, la primera ha de ser distinta de cero; esto constituye una restricción. Pensemos según la modelización II. Las posiciones de las cifras hacen de recipientes, distinguibles, 3 en total; los objetos, indistinguibles, son cifras unos, 9 en total. Lo primero, satisfacemos la restricción; así, ponemos un objeto en el primer recipiente, quedando 8 objetos por distribuir. Por otra parte, observemos que al ser números decimales, cada una de sus cifras debe ser menor que 10, lo cual se satisface pues el mayor valor sólo podría alcanzarse en su primera cifra, correspondiendo al número natural 900. En definitiva, cada número está representado por una distribución de 8 objetos indistinguibles (8 unos) en 3 recipientes distinguibles —900 lo está por 9 unos en el primer recipiente y ningún uno en el resto—. Por lo tanto, esta cuestión equivale a preguntarnos cuántas de tales distribuciones existen. Al ser los objetos indistinguibles, el orden de éstos en los recipientes no influye en el recuento de distribuciones; en otras palabras, se trata de una distribución no ordenada. Como puede haber recipientes con más de un objeto y puede haberlos vacíos, no hay restricciones para la aplicación de los objetos en los recipientes. Es por todo ello que el número de distribuciones es $CR(3, 8)$. ■

Actividad 19.16

Pensemos los dos ejemplos anteriores según la modelización I.

Ejemplo 663

¿Cuántos números vigesicuaternarios (base 24) de siete cifras son tales que sus cifras suman veintitrés?

[Cubit 143b].

Resolución.— Las cifras en el sistema de numeración vigesicuaternario son 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, H, I, J, K, L, M y N. Para que el número sea de siete cifras, la primera ha de ser distinta de cero; esto constituye una restricción. Pensemos según la modelización II. Las posiciones de las cifras hacen de recipientes, distinguibles, 7 en total; los objetos, indistinguibles, son cifras unos, 23 en total —las letras con valores respectivos desde A a N, de 10 a 23, en sus correspondientes codificaciones unarias—. Lo primero, satisfacemos la restricción; así, ponemos un objeto en el primer recipiente, quedando 22 objetos por distribuir. Por otra parte, observemos que al ser números vigesicuaternarios, cada una de sus cifras debe ser menor que 24, lo cual se satisface pues el mayor valor sólo podría alcanzarse en su primera cifra, correspondiendo al número vigesicuaternario N000000. En definitiva, cada número está representado por una distribución de 22 objetos indistinguibles (22 unos) en 7 recipientes distinguibles —N000000 lo está por 23 unos en el primer recipiente y ningún uno en el resto—. Por lo tanto, esta cuestión equivale a preguntarnos cuántas de tales distribuciones existen. Al ser los objetos indistinguibles, el orden de éstos en los recipientes no influye en el recuento de distribuciones; en otras palabras, se trata de una distribución no ordenada. Como puede haber recipientes con más de un objeto y puede haberlos vacíos, no hay restricciones para la aplicación de los objetos en los recipientes. Es por todo ello que el número de distribuciones es $CR(7, 22)$. ■

Actividad 19.17

¿Cuántos números naturales de siete cifras son tales que sus cifras suman veintitrés?

Nuevas operaciones combinatorias: S, Σ, p y Π

Definimos, e interpretamos ahora en la modelización II, las *nuevas operaciones combinatorias (menos simples)* que aparecen en el cuadro n.º 2a —teorema 19.47 (pág. 1198 de esta edición)—, S, Σ, p y Π, de la siguiente forma:

a) $S(k,r) = \frac{1}{r!}\sum_{i=0}^{r-1}(-1)^i\binom{r}{i}(r-i)^k$, $(\forall k, r \in \mathbb{N}, r \leq k)$ (**números de Stirling de segunda especie**) —satisfacen la recurrencia $S(k,r) = r \cdot S(k-1,r) + S(k-1,r-1)$ $(1 \leq r < k)$, con $S(0,0) = 1$, $S(k,0) = S(0,k) = 0$ $(k > 0)$ y $S(k,1) = S(n,n) = 1$—; interpretamos $S(k,n)$ como el número de distribuciones no ordenadas en las que cada recipiente contiene al menos un objeto (no admitimos recipientes vacíos) de k objetos distinguibles en n recipientes indistinguibles;

b) $\Sigma(k,n) = \sum_{i=1}^{n} S(k,i)$, que interpretamos como el número de distribuciones no ordenadas cualesquiera (admitimos recipientes vacíos) de k objetos distinguibles en n recipientes indistinguibles[25];

c) $p(k,r)$ (**función de partición positiva**[26]); satisfacen la recurrencia $p(k,r) = p(k-1,r-1) + p(k-r,r)$ $(1 < r < k)$, con $p(0,0) = 1$ y $p(k,1) = p(n,n) = 1$ $(1 \leq k,n)$; interpretamos $p(k,n)$ como el número de distribuciones no ordenadas en las que cada recipiente contiene al menos un objeto (no admitimos recipientes vacíos) de k objetos indistinguibles en n recipientes indistinguibles;

d) $\Pi(k,n) = \sum_{i=1}^{n} p(k,i)$ (**función de partición no negativa**), que interpretamos como el número de distribuciones no ordenadas cualesquiera (admitimos recipientes vacíos) de k objetos indistinguibles en n recipientes indistinguibles; $\Pi(n,n)$ suele designarse por $p(n)$.

Observación 19.3.1.— En algunos textos, $\Sigma(k,n)$ y $\Pi(k,n)$, se notan por $S(k)$ y $p(k)$, respectivamente. Por otro lado, $p(k,r)$ también se nota $p_k(r)$.

Distribuciones ordenadas

El siguiente teorema muestra los ocho tipos de distribuciones simples ordenadas y el número de distribuciones para cada tipo.

Como hemos dicho, por *distribución ordenada* nos referimos a que el orden de los objetos dentro de los recipientes es un elemento diferenciador entre distribuciones, esto es, que dos distribuciones son distintas si tales órdenes son distintos.

[25] La operación combinatoria $\Sigma(k,k)$ es conocida como el **número de Bell** B_k (*cfr. v. gr.* https://en.wikipedia.org/wiki/Bell_number).

[26] Interpretaremos la operación combinatoria $p(k,r)$ como número de particiones de un multiconjunto (modelización III) o de un número entero positivo (modelización IV), de ahí este nombre.

Teorema 19.48 (Modelización II: esquema de interpretaciones: distribuciones ordenadas)

Cuadro n.º 2.b
Los ocho tipos de distribuciones simples ordenadas de k objetos en n recipientes

Distribución	Objetos	Recipientes	Aplicación	N.º de distribuciones
Ordenada	Distinguibles	Distinguibles	Cualquiera	$P(k)CR(n,k)$
			Inyectiva	$V(n,k)$
			Sobreyectiva	$P(n)L(k,n)$
			Biyectiva	$P(n)$
		Indistinguibles	Cualquiera	$A(k,n)$
			Inyectiva	1
			Sobreyectiva	$L(k,n)$
			Biyectiva	1

Nuevas operaciones combinatorias: L y A

Definimos, e interpretamos ahora en la modelización II, las *nuevas operaciones combinatorias (menos simples)* que aparecen en el cuadro n.º 2b —teorema 19.48 (pág. 1202 de esta edición)—, L y A, de la siguiente forma:

a) $L(k,r) = \frac{k!}{r!}\binom{k-1}{r-1}$ (**números de Lah sin signo** [también llamados números de Stirling de tercera especie]); interpretamos $L(k,n)$ como el número de distribuciones ordenadas en las que cada recipiente contiene al menos un objeto (no admitimos recipientes vacíos) de k objetos distinguibles en n recipientes indistinguibles;

b) $A(k,n) = \sum_{i=1}^{n} L(k,i)$, que interpretamos como el número de distribuciones ordenadas cualesquiera (admitimos recipientes vacíos) de k objetos distinguibles en n recipientes indistinguibles.

Observación 19.3.2.— En algunos textos, $A(k,n)$ se nota por $L(k)$.

Teorema 19.49

Se satisface:

0. $P(k)CR(n,k) = V(n+k-1,k)$;
1. $P(n)L(k,n) = P(k)C(k-1,n-1)$;
2. $n^{\overline{k}} = \sum_{r=1}^{k} L(k,r)n^{\underline{k}}$.

Interpretación intermodal

El teorema 19.50 (pág. 1203 de esta edición) establece la correspondencia entre el modelo de distribución y el de selección, sirviendo de diccionario a la hora de traducir situaciones.

Por ejemplo, una distribución no ordenada de k objetos indistinguibles en n recipientes distinguibles donde ningún recipiente contiene más de un objeto (la aplicación subyacente es inyectiva), corresponde a una selección o muestra no ordenada de k objetos, procedente de un muestreo sin reemplazamiento de n objetos distinguibles.

Pero hemos de tener cuidado. Esta *intertraducción* no es ni completa ni unívoca:

- no es completa porque existen problemas de distribución (la subclase correspondiente a recipientes indistinguibles) intraducibles a problemas de selección, y
- no es unívoca porque, aunque todo problema de selección puede traducirse al menos a uno de distribución, algunos problemas de selección ordenada se traducen tanto a un problema de distribución ordenada como no ordenada de objetos distinguibles en recipientes distinguibles.

Teorema 19.50 (Modelizaciones I y II: diccionario intermodal)

Cuadro n.º 3 (primer diccionario intermodal)

Correspondencia entre el modelo de distribución simple y el de selección simple

Distribución de k objetos en n recipientes		Selección de k objetos de un total de n objetos distinguibles	
k objetos (a colocar)	Distinguibles	k objetos (muestra)	Selección ordenada
	Indistinguibles		Selección no ordenada
n recipientes	Distinguibles	n objetos	Distinguibles
	Indistinguibles		-
Aplicación	Cualquiera	Selección	Con reemplazamiento
	Inyectiva		Sin reemplazamiento
	Sobreyectiva		Con reemplazamiento
	Biyectiva		Sin reemplazamiento

§ 19.3.2 Modelización III. Partición simple de un conjunto

Se trata de las formas simples en que se puede partir un conjunto S de k elementos en n subconjuntos; cada una de estas formas simples es una colección $\{S_0, S_1, \ldots, S_{n-1}\}$ de subconjuntos de S que sea una partición de S.

Aunque hablamos de conjunto y subconjuntos, debemos entender multiconjunto y multisubconjuntos cuando se trate de elementos indistinguibles.

Siendo E y S los conjuntos de elementos y subconjuntos, respectivamente, el tipo de la aplicación $f : E \longrightarrow S$ representa la situación de los subconjuntos con respecto a los elementos —*cfr. infra* teorema 19.56 (pág. 1210 de esta edición)—).

Teorema 19.51 (Modelización III: estado de los subconjuntos y tipo de aplicación)

Cuadro n.º 1.bis
Correspondencia entre la situación de los n subconjuntos
y el tipo de la aplicación, $f : E \longrightarrow S$, de los k elementos en los n subconjuntos

Situación de los n subconjuntos	Tipo de $f : E \longrightarrow S$
Puede haber algunos vacíos o no unitarios	Cualquiera
Sólo hay vacíos o unitarios	Inyectiva ($k \leq n$)
Todos no vacíos	Sobreyectiva ($k \geq n$)
Todos unitarios	Biyectiva ($k = n$)

Partición en subconjuntos no ordenados

Una *partición ordenada* de un conjunto X, la entendemos como totalmente ordenada, siendo entonces admisible representarla, digamos que es una partición en n subconjuntos, por una tupla enádica $\langle X_0, X_1, \ldots, X_{n-1}\rangle$ (en realidad, los elementos son conjuntos o multiconjuntos) (los elementos de éstos no tienen por qué estar ordenados).

El siguiente teorema muestra los 16 tipos de particiones en subconjuntos no ordenados y el número de particiones para cada tipo.

Teorema 19.52 (Modelización III: esquema de interpretaciones: subconjuntos no ordenados)

Cuadro n.º 4.a
Los 16 tipos de particiones simples de un conjunto de k elementos en n subconjuntos no ordenados

Subconjuntos	Elementos	Particiones	Subconjuntos	N.º de particiones
No ordenados	Distinguibles	Ordenadas (tuplas)	$\exists$ vacíos o no unitarios	$VR(n,k)$
			Sólo vacíos o unitarios	$V(n,k)$
			Todos no vacíos	$P(n)S(k,n)$
			Todos unitarios	$P(n)$
		No ordenadas	$\exists$ vacíos o no unitarios	$\Sigma(k,n)$
			Sólo vacíos o unitarios	1
			Todos no vacíos	$S(k,n)$
			Todos unitarios	1
	Indistinguibles	Ordenadas (tuplas)	$\exists$ vacíos o no unitarios	$CR(n,k)$
			Sólo vacíos o unitarios	$C(n,k)$
			Todos no vacíos	$CR(n,k-n)$
			Todos unitarios	1
		No ordenadas	$\exists$ vacíos o no unitarios	$\Pi(k,n)$
			Sólo vacíos o unitarios	1
			Todos no vacíos	$p(k,n)$
			Todos unitarios	1

A continuación, algo más sobre particiones ordenadas.

Teorema 19.53
Si un conjunto A tiene n elementos y si $n_0 + n_1 + \cdots + n_{k-1} = n$, entonces hay $PR(n_0, n_1, \ldots, n_{k-1})$ particiones ordenadas $A_0, A_1, \ldots, A_{k-1}$, de A, con $|A_i| = n_i$, para $0 \leq i < k$.

Ejemplo 664

Sea Σ un alfabeto de 20 letras. ¿De cuántas maneras podemos obtener tres conjuntos disjuntos de letras de tal forma que los conjuntos tengan cardinales 3, 5 y 7, respectivamente?

Resolución.— Esto se reduce a contar particiones ordenadas, digamos A, B, C y D, de Σ, tales que $|A| = 3$, $|B| = 5$, $|C| = 7$ y $|D| = 5$ (este último está formado por las letras que no están ni en A ni en B ni en C). Existen $PR(3, 5, 7, 5)$ formas posibles. ■

Partición en subconjuntos ordenados

Un *subconjunto ordenado*, lo entendemos como totalmente ordenado, siendo entonces admisible representarlo, digamos que tiene n elementos, por una tupla enádica $\langle x_0, x_1, \ldots, x_{n-1} \rangle$.

El siguiente teorema muestra los ocho tipos de particiones en subconjuntos ordenados y el número de particiones para cada tipo.

Teorema 19.54 (Modelización III: esquema de interpretaciones: subconjuntos ordenados)

Cuadro n.º 4.b

Los 8 tipos de particiones simples de un conjunto de k elementos en n subconjuntos ordenados

Subconjuntos	Elementos	Particiones	Subconjuntos	N.º de particiones
Ordenados (tuplas)	Distinguibles	Ordenadas (tuplas)	∃ vacíos o no unitarios	$P(k)CR(n, k)$
			Sólo vacíos o unitarios	$V(n, k)$
			Todos no vacíos	$P(n)L(k, n)$
			Todos unitarios	$P(n)$
		No ordenadas	∃ vacíos o no unitarios	$A(k, n)$
			Sólo vacíos o unitarios	1
			Todos no vacíos	$L(k, n)$
			Todos unitarios	1

Interpretación de las operaciones combinatorias menos simples

El teorema 19.52 (pág. 1205 de esta edición) recoge las interpretaciones en esta modelización III de las operaciones combinatorias simples y menos simples. A modo de ejemplo, las menos simples.

$S(k, n)$

Lo interpretamos como el número de particiones simples no ordenadas de un conjunto de k elementos (distinguibles) en n subconjuntos no ordenados y no vacíos.

Ejemplo 665

¿Cuántas son las particiones simples no ordenadas del conjunto $\{a, b, c, d\}$ en dos subconjuntos no ordenados y no vacíos? ¿Cuáles son?

Resolución.— El número de particiones simples no ordenadas del conjunto $\{a, b, c, d\}$ de $k = 4$ elementos (distinguibles) en $n = 2$ subconjuntos no ordenados y no vacíos es $S(4, 2) = 7$; en efecto, estas particiones son: $\{\{a\}, \{b, c, d\}\}$, $\{\{b\}, \{a, c, d\}\}$, $\{\{c\}, \{a, b, d\}\}$, $\{\{d\}, \{a, b, c\}\}$, $\{\{a, b\}, \{c, d\}\}$, $\{\{a, c\}, \{b, d\}\}$ y $\{\{a, d\}, \{b, c\}\}$. ■

$\Sigma(k, n)$

Lo interpretamos como el número de particiones simples no ordenadas de un conjunto de k elementos distinguibles en n subconjuntos no ordenados, pudiendo ser éstos vacíos o unitarios.

Ejemplo 666

¿Cuántas son las particiones simples no ordenadas del conjunto $\{a, b, c, d\}$ en dos subconjuntos no ordenados, pudiendo ser éstos vacíos o no unitarios? ¿Cuáles son?

Resolución.— El número de particiones simples no ordenadas del conjunto $\{a, b, c, d\}$ de $k = 4$ elementos (distinguibles) en $n = 2$ subconjuntos no ordenados, vacíos y no unitarios es $\Sigma(4, 2) = \sum_{i=1}^{2} S(4, i) = S(4, 1) + S(4, 2) = 1 + 7 = 8$; en efecto, estas particiones son: $\{\emptyset, \{a, b, c, d\}\}$, $\{\{a\}, \{b, c, d\}\}$, $\{\{b\}, \{a, c, d\}\}$, $\{\{c\}, \{a, b, d\}\}$, $\{\{d\}, \{a, b, c\}\}$, $\{\{a, b\}, \{c, d\}\}$, $\{\{a, c\}, \{b, d\}\}$ y $\{\{a, d\}, \{b, c\}\}$. ■

$p(k, n)$

Lo interpretamos como el número de particiones simples no ordenadas de un multiconjunto de k elementos indistinguibles en n submulticonjuntos no ordenados y no vacíos.

Ejemplo 667

¿Cuántas son las particiones simples no ordenadas del multiconjunto $\{\{1, 1, 1, 1, 1\}\}$ en dos submulticonjuntos no ordenados y no vacíos? ¿Cuáles son?

Resolución.— El número de particiones simples no ordenadas del multiconjunto $\{\{1, 1, 1, 1, 1\}\}$ de $k = 5$ elementos indistinguibles en $n = 2$ submulticonjuntos no ordenados y no vacíos es $p(5, 2) = 2$; en efecto, estas particiones son: $\{\{\{\{1\}\}, \{\{1, 1, 1, 1\}\}\}\}$ y $\{\{\{\{1, 1\}\}, \{\{1, 1, 1\}\}\}\}$. ■

$\Pi(k, n)$

Lo interpretamos como el número de particiones simples no ordenadas de un multiconjunto de k elementos indistinguibles en n submulticonjuntos no ordenados, pudiendo ser éstos vacíos o no unitarios.

Ejemplo 668

¿Cuántas son las particiones simples no ordenadas del multiconjunto $\{\{1,1,1,1,1\}\}$ en dos submulticonjuntos no ordenados, pudiendo ser éstos vacíos o no unitarios? ¿Cuáles son?

Resolución.— El número de particiones simples no ordenadas del multiconjunto $\{\{1,1,1,1,1\}\}$ de $k = 5$ elementos indistinguibles en $n = 2$ submulticonjuntos no ordenados, vacíos y no unitarios es $\Pi(5,2) = \sum_{i=1}^{2} p(5,i) = p(5,1) + p(5,2) = 1 + 2 = 3$; en efecto, estas particiones son: $\{\{\emptyset, \{\{1,1,1,1,1\}\}\}\}$, $\{\{\{\{1\}\}, \{\{1,1,1,1\}\}\}\}$ y $\{\{\{\{1,1\}\}, \{\{1,1,1\}\}\}\}$. ■

$L(k,n)$

Lo interpretamos como el número de particiones simples no ordenadas de un conjunto de k elementos (distinguibles) en n subconjuntos ordenados y no vacíos.

Ejemplo 669

¿Cuántas son las particiones simples no ordenadas del conjunto $\{0,1,2\}$ en dos subconjuntos ordenados y no vacíos? ¿Cuáles son?

Resolución.— El número de particiones simples no ordenadas del conjunto $\{0,1,2\}$ de $k = 3$ elementos (distinguibles) en $n = 2$ subconjuntos ordenados y no vacíos es $L(3,2) = 6$; en efecto, estas particiones son: $\{\langle 0\rangle, \langle 1,2\rangle\}$, $\{\langle 0\rangle, \langle 2,1\rangle\}$, $\{\langle 1\rangle, \langle 0,2\rangle\}$, $\{\langle 1\rangle, \langle 2,0\rangle\}$, $\{\langle 2\rangle, \langle 0,1\rangle\}$ y $\{\langle 2\rangle, \langle 1,0\rangle\}$. ■

$A(k,n)$

Lo interpretamos como el número de particiones simples no ordenadas de un conjunto de k elementos (distinguibles) en n subconjuntos ordenados, pudiendo ser éstos vacíos o no unitarios.

Ejemplo 670

¿Cuántas son las particiones simples no ordenadas del conjunto $\{0,1,2\}$ en dos subconjuntos ordenados, pudiendo ser éstos vacíos o no unitarios? ¿Cuáles son?

Resolución.— El número de particiones simples no ordenadas del conjunto $\{0,1,2\}$ de $k = 3$ elementos (distinguibles) en $n = 2$ subconjuntos ordenados, vacíos y no unitarios es $A(3,2) = \sum_{i=1}^{2} L(3,i) = L(3,1) + L(3,2) = 3! + 6 = 12$; en efecto, estas particiones son: $\{\emptyset, \langle 0,1,2\rangle\}$, $\{\emptyset, \langle 0,2,1\rangle\}$, $\{\emptyset, \langle 1,0,2\rangle\}$, $\{\emptyset, \langle 1,2,0\rangle\}$, $\{\emptyset, \langle 2,0,1\rangle\}$, $\{\emptyset, \langle 2,1,0\rangle\}$, $\{\langle 0\rangle, \langle 1,2\rangle\}$, $\{\langle 0\rangle, \langle 2,1\rangle\}$, $\{\langle 1\rangle, \langle 0,2\rangle\}$, $\{\langle 1\rangle, \langle 2,0\rangle\}$, $\{\langle 2\rangle, \langle 0,1\rangle\}$ y $\{\langle 2\rangle, \langle 1,0\rangle\}$. ■

Interpretación intermodal

El teorema 19.55 (pág. 1209 de esta edición) establece la correspondencia entre el modelo de partición simple de un conjunto y el de distribución simple, sirviendo de diccionario a la hora de traducir situaciones.

En este caso,

- la *intertraducción* es completa y unívoca, y
- aunque hablemos de conjunto y subconjuntos, debemos entender *multiconjunto* y *submulticonjuntos* cuando se trate de elementos indistinguibles.

Teorema 19.55 (Modelizaciones II y III: diccionario intermodal)

Cuadro n.º 5 (segundo diccionario intermodal)
Correspondencia entre el modelo de distribución simple y el de partición simple

Distribución de k objetos en n recipientes		Partición de un conjunto de k elementos en n subconjuntos	
Distribución	Ordenada	Subconjuntos	Ordenados
	No ordenada		No ordenados
Objetos	Distinguibles	Elementos	Distinguibles
	Indistinguibles		Indistinguibles
Recipientes	Distinguibles	Partición	Ordenada
	Indistinguibles		No ordenada
Aplicación	Cualquiera	Subconjuntos	Vacíos y no unitarios
	Inyectiva		Vacíos y unitarios
	Sobreyectiva		No vacíos
	Biyectiva		Unitarios

§ 19.3.3 Modelización IV. Descomposición simple de un entero positivo

Se trata de las formas simples en que se puede descomponer, esto es, partir, particionar, un entero positivo k en n sumandos enteros no negativos; tal descomposición es cualquier tupla, ordenada o no, de enteros no negativos $\langle k_1, k_2, \ldots, k_n \rangle \in \mathbb{N}^n$ tal que $k = k_1 + k_2 + \cdots + k_n$.

Un entero positivo k es una colección de k objetos indistinguibles, concretamente de k unos: $k = k_1 + k_2 + \cdots + k_n = (1 + \overset{k_1}{\cdots} + 1) + (1 + \overset{k_2}{\cdots} + 1) + \cdots + (1 + \overset{k_n}{\cdots} + 1)$.

Teorema 19.56 (Modelización IV: estado de los sumandos y tipo de aplicación)

Cuadro n.º 1.*ter*
Correspondencia entre la situación de los n sumandos
y el tipo de la aplicación, $f : U \longrightarrow M$, de los k unos en los n sumandos

Situación de los n sumandos	Tipo de $f : U \longrightarrow M$
Todos no negativos	Cualquiera
Sólo ceros o unos	Inyectiva ($k \leq n$)
Todos positivos	Sobreyectiva ($k \geq n$)
Todos uno	Biyectiva ($k = n$)

Teorema 19.57 (Modelización IV: esquema de interpretaciones)

Cuadro n.º 6
Los ocho tipos de descomposiciones simples de un entero positivo k en n sumandos enteros no negativos

Descomposición	Sumandos	N.º de descomposiciones
Ordenada (tuplas)	Todos no negativos	$CR(n, k)$
	Sólo ceros o unos	$C(n, k)$
	Todos positivos	$CR(n, k - n)$
	Todos uno	1
No ordenada	Todos no negativos	$\Pi(k, n)$
	Sólo ceros o unos	1
	Todos positivos	$p(k, n)$
	Todos uno	1

Observación 19.3.3.— La *descomposición ordenada* la entendemos como totalmente ordenada, entonces, como sabemos, es admisible representarla, digamos que tiene n elementos, por una tupla enádica $\langle k_0, k_1, \ldots, k_{n-1} \rangle$ (los elementos son los sumandos).

A modo de ejemplos aclaratorios:

- descomposición ordenada: $\triangle + \square \neq \square + \triangle$;
- descomposición no ordenada: $\triangle + \square = \square + \triangle$;
- sumandos no negativos: por ejemplo, $2 = 2+0+0 = 0+2+0 = 0+0+2 = 1+1+0 = 1+0+1 = 0+1+1$;
- sumandos 0 o 1: por ejemplo, $2 = 0+1+1 = 1+0+1 = 1+1+0$;

- sumandos positivos: por ejemplo, $4 = 1 + 1 + 2 = 1 + 2 + 1 = 2 + 1 + 1$;
- sumandos 1: por ejemplo, $3 = 1 + 1 + 1$.

Sobre la interpretación

El teorema 19.57 (pág. 1210 de esta edición) recoge las interpretaciones en esta modelización IV de algunas operaciones combinatorias simples y menos simples. A modo de ejemplo, las de p y Π.

$p(k, n)$

Lo interpretamos como el número de descomposiciones simples no ordenadas de un entero positivo k en n sumandos enteros positivos.

Ejemplo 671

¿Cuántas son las descomposiciones simples no ordenadas del número 5 en dos sumandos enteros positivos? ¿Cuáles son?

Resolución.— El número de descomposiciones simples no ordenadas del entero positivo $k = 5$ en $n = 2$ sumandos enteros positivos es $p(5, 2) = 2$; en efecto, estas descomposiciones son: $1 + 4$ y $2 + 3$. ■

$\Pi(k, n)$

Lo interpretamos como el número de descomposiciones simples no ordenadas de un entero positivo k en n sumandos enteros no negativos.

Ejemplo 672

¿Cuántas son las descomposiciones simples no ordenadas del número 5 en dos sumandos enteros no negativos? ¿Cuáles son?

Resolución.— El número de descomposiciones simples no ordenadas del entero positivo $k = 5$ en $n = 2$ sumandos enteros no negativos es $\Pi(5, 2) = \sum_{i=1}^{2} p(5, i) = p(5, 1) + p(5, 2) = 1 + 2 = 3$; en efecto, estas descomposiciones son: $0 + 5$, $1 + 4$ y $2 + 3$. ■

Interpretación intermodal

El teorema 19.58 (pág. 1212 de esta edición) establece la correspondencia entre el modelo de descomposición simple de un entero positivo y el de distribución simple.

Por ejemplo, la descomposición de un número entero positivo k en n sumandos positivos, puede interpretarse como la distribución no ordenada de k objetos indistinguibles en n recipientes distin-

guibles donde ningún recipiente queda vacío (la aplicación subyacente es sobreyectiva), y recíprocamente.

Y si nos ayudamos del segundo diccionario intermodal como la partición ordenada de un conjunto de k elementos indistinguibles en n subconjuntos no ordenados y no vacíos.

La *intertraducción* es completa y unívoca entre las distribuciones simples no ordenadas de k objetos indistinguibles en n recipientes y las descomposiciones simples de un entero positivo k en n sumandos enteros no negativos.

Teorema 19.58 (Modelizaciones II y IV: diccionario intermodal)

Cuadro n.º 7 (tercer diccionario intermodal)
Correspondencia entre el modelo de distribución y el de descomposición

Distribución simple no ordenada de k objetos indistinguibles en n recipientes		Descomposición simple de un entero positivo k en n sumandos enteros no negativos	
Recipientes	Distinguibles	Descomposición	Ordenada
	Indistinguibles		No ordenada
Aplicación	Cualquiera	Sumandos	No negativos
	Inyectiva		0 y 1
	Sobreyectiva		Positivos
	Biyectiva		1

§ 19.3.4 Abundando en la interpretación intermodal

Utilizando los diccionarios intermodales presentados en el capítulo y a modo de ejemplo de interpretación intermodal, fijémonos en los siguientes ejemplos.

Ejemplo 673

Interpretemos la descomposición ordenada de un número entero positivo k en n sumandos enteros positivos en las modelizaciones en las que tenga sentido hacerlo.

Resolución.— Modelizaciones:

II. La distribución no ordenada de k objetos indistinguibles en n recipientes distinguibles con la condición de que ningún recipiente quede vacío.

III. La partición ordenada de un conjunto de k elementos indistinguibles en n subconjuntos no ordenados y no vacíos. ■

Destacamos, en particular, las diferentes interpretaciones, tanto para las operaciones combinatorias simples V, VR, P, C y CR (cálculo del número de variaciones, permutaciones y combinaciones, sin y con repetición), como para las operaciones combinatorias menos simples S, p, L, Σ, Π y A, en las diferentes modelizaciones en las que tengan sentido.

A modo de ejemplos, las de V, C y Π.

Ejemplo 674

Interpretemos $V(n,k)$ en las modelizaciones en las que tenga sentido hacerlo.

Resolución.— Modelizaciones:

I. Número de muestras ordenadas sin reemplazamiento de k objetos de un total de n objetos distinguibles.

II. Número de distribuciones de k objetos distinguibles en n recipientes distinguibles con la condición de que ningún recipiente contenga más de un objeto.

III. Número de particiones ordenadas de un conjunto de k elementos distinguibles en n subconjuntos entre los que los hay vacíos y unitarios. ■

Ejemplo 675

Interpretemos $C(n,k)$ en las modelizaciones en las que tenga sentido hacerlo.

Resolución.— Modelizaciones:

I. Número de muestras no ordenadas sin reemplazamiento de k objetos de un total de n objetos distinguibles.

II. Número de distribuciones de k objetos indistinguibles en n recipientes distinguibles con la condición de que ningún recipiente contenga más de un objeto.

III. Número de particiones ordenadas de un conjunto de k elementos indistinguibles en n subconjuntos entre los que los hay vacíos y unitarios.

IV. Número de descomposiciones ordenadas de un entero positivo k en n sumandos entre los que sólo hay ceros y unos. ■

Ejemplo 676

Interpretemos $\Pi(k,n)$ en las modelizaciones en las que tenga sentido hacerlo.

Resolución.— Modelizaciones:

II. Número de distribuciones no ordenadas de k objetos indistinguibles en n recipientes indistinguibles pudiendo haber recipientes vacíos o con más de un objeto.

III. Número de particiones no ordenadas de un conjunto de k elementos indistinguibles en n subconjuntos entre los que los hay vacíos y no unitarios.

IV. Número de descomposiciones no ordenadas de un entero positivo k en n sumandos no negativos. ■

Actividad 19.18

Compendiemos las diferentes interpretaciones para el resto de operaciones combinatorias.

[SEL 11:7].

Las actividades 19.18 y 19.19 (págs. 1214 y 1214 de esta edición) podrían, o incluso deberían, ser imperativas para quienes estudiamos con inquietud; la primera contribuirá a que dispongamos de modelos que nos permitan identificar similitudes en futuras cuestiones, a la vez que nos sirvan de ayuda en su resolución; la segunda incrementará nuestra experiencia en el rigor de la demostración.

Actividad 19.19

Interpretemos con las definiciones y con las cuatro modelizaciones los teoremas 19.3, 19.7, 19.8, 19.9 y 19.10 (págs. 1130, 1132, 1133, 1133 y 1133 de esta edición), esto es, realicemos una demostración combinatoria de ellas (sin usar los conceptos, ni de número factorial ni de número factorial descendente ni de número factorial ascendente).

[Cubit 146], [Cubit 147], [EFO 27.5.2025:7], [EFE 18.6.2025:7].

Con miras a su resolución.— A modo de ejemplos de lo que hemos de hacer en la actividad anterior, los dos siguientes: I., acerca del cardinal del conjunto potencia —*cfr. supra* teorema 19.8.12 (pág. 1133)—, $\forall n \in \mathbb{N}$, $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$, igualdad cierta, pues, para un conjunto de cardinal n, a la izquierda de la igualdad vemos la suma del número de subconjuntos de cardinal cero más el número de subconjuntos de cardinal uno, y así sucesivamente, más el número de subconjuntos de cardinal n, mientras que a la derecha vemos el número de subconjuntos de un conjunto de cardinal n, y II., la igualdad —*cfr. supra* teorema 19.11.21 (pág. 1134)—, $\forall n \in \mathbb{N}, \forall k \in \mathbb{N}\backslash\{0,1\}$, $\binom{n+2}{k} = \binom{n}{k} + 2\cdot\binom{n}{k-1} + \binom{n}{k-2}$, es cierta; en efecto, por una parte, $\binom{n+2}{k}$ es el número de subconjuntos de cardinal k de un conjunto de cardinal $n+2$; por otra, fijémonos en cómo contar sus subconjuntos de cardinal k: sea $C = \{a, b, c_1, c_2, \ldots, c_n\}$ un conjunto de cardinal $n+2$, contemos sus subconjuntos de cardinal k vía el principio de la adición distinguiendo los sucesos: $S \leftrightharpoons$ ser un subconjunto de C de cardinal k; $S_0 \leftrightharpoons$ ser un subconjunto de C de cardinal k al que no pertenece ni a ni b; $S_1 \leftrightharpoons$ ser un subconjunto de C de cardinal k al que pertenece a y no pertenece b; $S_2 \leftrightharpoons$ ser un subconjunto de C de cardinal k al que no pertenece a y sí pertenece b; $S_3 \leftrightharpoons$ ser

un subconjunto de C de cardinal k al que pertenecen a y b; claramente estos sucesos son incompatibles y $S = S_0 \cup S_1 \cup S_2 \cup S_3$ (implícitamente, hemos usado la eliminación de la disyunción [Cas/ED] partiendo el espacio en estos sucesos [en lenguaje de la lógica de juntores: $(\neg a \wedge \neg b) \veebar (a \wedge \neg b) \veebar (\neg a \wedge b) \veebar (a \wedge b)$]); los números de formas en que suceden estos sucesos (interpretadas según la modelización I) son: $\#S_0 = \binom{n}{k}$ (n.º de selecciones simples sin reposición de k elementos de $C \setminus \{a, b\}$), $\#S_1 = \binom{n}{k-1}$ (n.º de selecciones simples sin reposición de $k-1$ elementos de $C \setminus \{a, b\}$ —$k-1$ porque a ya está en el subconjunto—), $\#S_2 = \binom{n}{k-1}$ (n.º de selecciones simples sin reposición de $k-1$ elementos de $C \setminus \{a, b\}$ —$k-1$ porque b ya está en el subconjunto—) y $\#S_3 = \binom{n}{k-2}$ (n.º de selecciones simples sin reposición de $k-2$ elementos de $C \setminus \{a, b\}$ —$k-2$ porque a y b ya están en el subconjunto—); por lo tanto, por el principio de la adición, el número de formas en que sucede S, $\#S$, esto es, $\binom{n+2}{k}$, es igual a $\binom{n}{k} + \binom{n}{k-1} + \binom{n}{k-1} + \binom{n}{k-2}$, justamente lo que perseguíamos demostrar.

§ 19.3.5 La ecuación diofántica $x_1 + x_2 + \ldots + x_n = k$ (Parte II)

Veamos ahora la interpretación de una solución entera no negativa de la ecuación $x_1 + x_2 + \ldots + x_n = k$ en los contextos de cada una de las cuatro modelizaciones.

En los ejemplos interpretaremos una solución no negativa de la ecuación $x_1 + x_2 + x_3 = 2$. Recordemos que esta ecuación tiene un total de $CR(3, 2) = C(3 + 2 - 1, 2) = 6$ soluciones no negativas.

Modelización I

Contexto de los problemas de selección simple.

Si la variable x_i representa el número de objetos de tipo i, una solución entera no negativa $(s_1, s_2, \ldots, s_n)$ de $x_1 + x_2 + \ldots + x_n = k$ corresponde a una selección (muestra) simple no ordenada de k objetos, procedente de un muestreo con reemplazamiento de n tipos distinguibles de objetos, en la que s_1 son de tipo x_1, s_2 son de tipo x_2, ..., s_n son de tipo x_n. El número total de estas selecciones es[27] $CR(n, k)$.

Ejemplo 677

Representemos en el contexto de los problemas de selección simple, todas las soluciones no negativas de $x_1 + x_2 + x_3 = 2$, en el orden $\langle 0, 0, 2\rangle$, $\langle 0, 2, 0\rangle$, $\langle 2, 0, 0\rangle$, $\langle 1, 1, 0\rangle$, $\langle 1, 0, 1\rangle$ y $\langle 0, 1, 1\rangle$.

Resolución.— Cada selección no ordenada con reemplazamiento de dos objetos de un total de tres objetos distinguibles, o_0, o_1 y o_2, corresponde a una solución no negativa de $x_1 + x_2 + x_3 = 2$; así,

[27] *Vid. supra* cuadro n.º 0 — teorema 19.45 (pág. 1191 de esta edición)—.

en el orden dado, dichas soluciones están representadas por las selecciones

$$(o_2, o_2),$$
$$(o_1, o_1),$$
$$(o_0, o_0),$$
$$(o_0, o_1),$$
$$(o_0, o_2),$$
$$(o_1, o_2).$$ ■

Modelización II

Contexto de los problemas de distribución simple.

Cada solución entera no negativa de $x_1 + x_2 + \ldots + x_n = k$ corresponde a una distribución simple de k objetos indistinguibles (en este caso, los k unos) en n recipientes distinguibles x_1, x_2, ..., x_n, interpretados como recipientes de unos (por ejemplo, interpretamos $x_i = p$ como que el recipiente i contiene p unos), distribución que es no ordenada (el orden de los objetos dentro de los recipientes no importa) y que no está sujeta a restricción alguna sobre la situación de los recipientes con respecto a los objetos (restricciones como si puede quedar alguno vacío o si no pueden contener más de un objeto). El número total de estas distribuciones es[28] $CR(n, k)$.

Ejemplo 678

Representemos en el contexto de los problemas de distribución simple, todas las soluciones no negativas de $x_1 + x_2 + x_3 = 2$, en el orden $\langle 0, 0, 2\rangle$, $\langle 0, 2, 0\rangle$, $\langle 2, 0, 0\rangle$, $\langle 1, 1, 0\rangle$, $\langle 1, 0, 1\rangle$ y $\langle 0, 1, 1\rangle$.

[Cubit 144].

Resolución.— Cada distribución no ordenada, no sujeta a condición alguna, de dos objetos indistinguibles, ✓y ✓, en tres recipientes distinguibles, R_1, R_2 y R_3, corresponde a una solución no negativa de $x_1 + x_2 + x_3 = 2$; así, en el orden dado, dichas soluciones están representadas por las distribuciones

R_1	R_2	R_3
		✓✓

,

R_1	R_2	R_3
	✓✓	

,

R_1	R_2	R_3
✓✓		

,

---

[28] *Vid. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—.

R_1 ✓	R_2 ✓	R_3

,

R_1 ✓	R_2	R_3 ✓

,

R_1	R_2 ✓	R_3 ✓

. ■

Modelización III

Contexto de los problemas de partición simple.

Cada solución entera no negativa de $x_1 + x_2 + \ldots + x_n = k$ corresponde a una partición simple ordenada de un multiconjunto de k elementos indistinguibles en n submulticonjuntos no ordenados donde puede haberlos vacíos y no unitarios. El número total de estas particiones es[29] $CR(n, k)$.

Ejemplo 679

Representemos en el contexto de los problemas de partición simple, todas las soluciones no negativas de $x_1 + x_2 + x_3 = 2$, en el orden $\langle 0, 0, 2\rangle$, $\langle 0, 2, 0\rangle$, $\langle 2, 0, 0\rangle$, $\langle 1, 1, 0\rangle$, $\langle 1, 0, 1\rangle$ y $\langle 0, 1, 1\rangle$.

[Cubit 148].

Resolución.— Sea el multiconjunto $\{\{\triangle, \triangle\}\}$, entonces cada partición ordenada suya de 2 elementos (indistinguibles) en 3 submulticonjuntos no ordenados donde los hay vacíos y no unitarios, corresponde a una solución no negativa de $x_1 + x_2 + x_3 = 2$; así, en el orden dado, dichas soluciones están representadas por las particiones

$$\begin{aligned}
&\langle \emptyset, \emptyset, \{\{\triangle, \triangle\}\}\rangle,\\
&\langle \emptyset, \{\{\triangle, \triangle\}\}, \emptyset\rangle,\\
&\langle \{\{\triangle, \triangle\}\}, \emptyset, \emptyset\rangle,\\
&\langle \{\{\triangle\}\}, \{\{\triangle\}\}, \emptyset\rangle,\\
&\langle \{\{\triangle\}\}, \emptyset, \{\{\triangle\}\}, \{\{\triangle\}\}\rangle.
\end{aligned}$$ ■

Observación 19.3.4.— $\{\{\triangle, \triangle\}\}$ es un multiconjunto de un elemento con multiplicidad dos; $\emptyset$ es el conjunto vacío; $\{\{\triangle\}\}$ es un multiconjunto de un elemento con multiplicidad uno; $\emptyset$, $\{\{\triangle\}\}$ y $\{\{\triangle, \triangle\}\}$ son los submulticonjuntos de $\{\{\triangle, \triangle\}\}$.

---

[29] *Vid. supra* cuadro n.º 4.a —teorema 19.52 (pág. 1205 de esta edición)—.

Observación 19.3.5.— Pudiésemos haber relajado algo la notación, ya que al tener un solo elemento, el multiconjunto $\{\{\triangle\}\}$ coincide con el conjunto $\{\triangle\}$, pero hemos preferido $\{\{\triangle\}\}$ por consistencia con ser una partición de submulticonjuntos.

Modelización IV

Contexto de los problemas de descomposición simple.

Cada solución entera no negativa de $x_1 + x_2 + \ldots + x_n = k$ corresponde a una descomposición simple ordenada del entero positivo k en n sumandos no negativos. El número total de estas descomposiciones es[30] $CR(n,k)$.

Ejemplo 680

Representemos en el contexto de los problemas de descomposición simple, todas las soluciones no negativas de $x_1 + x_2 + x_3 = 2$, en el orden $\langle 0,0,2\rangle$, $\langle 0,2,0\rangle$, $\langle 2,0,0\rangle$, $\langle 1,1,0\rangle$, $\langle 1,0,1\rangle$ y $\langle 0,1,1\rangle$.

[Cubit 149].

Resolución.— Cada descomposición ordenada del entero positivo 2 en tres sumandos no negativos corresponde a una solución no negativa de $x_1 + x_2 + x_3 = 2$; así, en el orden dado, dichas soluciones están representadas por las descomposiciones

$$\begin{aligned} 2 &= 0+0+2 \\ &= 0+2+0 \\ &= 2+0+0 \\ &= 1+1+0 \\ &= 1+0+1 \\ &= 0+1+1. \end{aligned}$$



Actividad 19.20

Interpretemos una solución entera positiva de la ecuación $x_1 + x_2 + \ldots + x_n = k$ en los contextos de cada una de las cuatro modelizaciones simples estudiadas.

---

[30] *Vid. supra* cuadro n.º 6 —teorema 19.57 (pág. 1210 de esta edición)—.

Ejemplo 681

¿De cuántas formas pudiésemos repartir 7 ejemplares del mismo libro en 3 cajas, X, Y y Z, de tal manera que al menos haya un ejemplar en cada caja y que en X haya igual o más ejemplares que en Y y en esta última igual o más ejemplares que en Z? (Los 7 ejemplares caben en cualquier caja).

Resolución.— Un enunciado equivalente en términos de la ecuación diofántica estudiada es el siguiente.

¿Cuántas soluciones (enteras) positivas tiene la ecuación diofántica $x_1 + x_2 + x_3 = 7$ con $x_3 \leq x_2 \leq x_1$?

Esta ecuación con esa restricción tiene $p(7,3) = 4$ soluciones positivas. Concretamente, estas cuatro soluciones son: $\langle 5,1,1\rangle$, $\langle 4,2,2\rangle$, $\langle 3,3,1\rangle$ y $\langle 3,2,2\rangle$. ■

Observación 19.3.6.— Estudiemos el caso $p(7,3)$ en alguna modelización compatible. Observemos que la restricción $x_3 \leq x_2 \leq x_1$ hace como si las variables fuesen indistinguibles; por ejemplo, en la modelización IV, $5+1+1$ es la misma descomposición que $1+5+1$ y $1+1+5$. Es decir, dicha restricción fuerza que sólo haya una posibilidad y eso equivale a que los recipientes sean indistinguibles.

Observación 19.3.7.— Fijémonos en el cuadro n.º 2.a (teorema 19.47 [pág. 1198 de esta edición]) y en el cuadro n.º 4.a (teorema 19.52 [pág. 1205 de esta edición]) e identifiquemos allí la situación del ejemplo anterior.

Podemos encontrar una tabla con los valores de p en Wikipedia: https://en.wikipedia.org/wiki/Triangle_of_partition_numbers.

Podemos visualizar este ejemplo en Wolfram|Alpha introduciendo:

```
particiones de 7 en 3 partes
```

§ 19.3.6 Ejemplos de las cuatro modelizaciones

Ejemplo 682 (PRen7)

En una prueba de rendimiento, ¿de cuántas formas puede un computador central c_0 repartir tres tareas indistinguibles entre siete computadores auxiliares, c_1, c_2, c_3, c_4, c_5, c_6 y c_7, si cualquiera de éstos puede recibir cualquier número de tareas?

[EFO 1.6.2017:5a], [EFE 7.7.2021:7], [SEP 12.5.2022], [EFO 20.5.2022:7a] (4 tareas, 3 computadores auxiliares, 15 formas).

Resolución.— En el ejemplo 649 (pág. 1180 de esta edición) demostramos que cada reparto de 3 tareas indistinguibles entre 7 computadores auxiliares distintos (en adelante, reparto) está representado por una aplicación del conjunto de éstos, $C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7\}$, en $\{0, 1, 2, 3\}$ tal que a cada computador auxiliar le asocia el número de tareas que le corresponden sujeta a la condición de que la suma de tales números es 3, por lo que el número de formas en las que c_0 puede repartir tres tareas idénticas entre siete computadores auxiliares sin ninguna restricción es el número de combinaciones con repetición $CR(7, 3) = C(7 + 3 - 1, 3) = 84$.

Centrémonos ahora en resolver la cuestión según se exige.

I. *Cálculo del recuento de acuerdo con la modelización I.*

Veámoslo ahora, por ejemplo, por la modelización I, considerando las entidades como los objetos en el lenguaje de esta modelización. Cada reparto está representado por una selección simple (muestra) de 3 objetos de $C = \{c_1, c_2, c_3, c_4, c_5, c_6, c_7\}$, esto es, de un total de 7 objetos distinguibles. La selección es no ordenada, pues el orden de los objetos en la muestra no importa para distinguir muestras; por ejemplo, los repartos (c_3, c_3, c_7), (c_3, c_7, c_3) y (c_7, c_3, c_3) son idénticos (se trata del mismo submulticonjunto $\{\{c_3, c_3, c_7\}\}$ del multiconjunto $\{\{c_1, \overset{3}{\ldots}, c_1, c_2, \overset{3}{\ldots}, c_2, \ldots, c_7, \overset{3}{\ldots}, c_7\}\}$). La selección es con reemplazamiento, ya que un computador auxiliar puede ser seleccionado más de una vez (puede recibir más de una tarea). Según lo estudiado (*cfr. supra* cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—), el número total de selecciones es $CR(7, 3) = C(7 + 3 - 1, 3) = (7 + 3 - 1)!/(3! \cdot (7 - 1)!) = 84$.

II. *Interpretación del resultado de acuerdo con cada una de las demás modelizaciones compatibles con la situación expuesta.*

- Las *modelizaciones compatibles* son las cuatro estudiadas. Veamos las interpretaciones según las que restan.
- *Interpretación de acuerdo con la modelización II.*

Cada reparto está representado por una distribución simple de 3 objetos indistinguibles (las tareas) en 7 recipientes distinguibles (los computadores), siendo cualquiera la aplicación del multiconjunto de objetos en el conjunto de recipientes. Por ejemplo, si ✓ designa una tarea indistinguible, el reparto (c_3, c_3, c_7) (submulticonjunto $\{\{c_3, c_3, c_7\}\}$) es la distribución no ordenada $\{\checkmark \longmapsto c_3, \checkmark \longmapsto c_3, \checkmark \longmapsto c_7\}$, gráficamente

c_1	c_2	c_3	c_4	c_5	c_6	c_7
		✓✓				✓

, que pudiésemos codificar en base 4 (son 3 objetos a repartir) por 0020001. Como vemos, la distribución es no ordenada, ya que por ser los objetos indistinguibles, el orden de los mismos en cada recipiente no importa para distinguir distribuciones.

- *Interpretación de acuerdo con la modelización III.*

  Cada reparto está representado por una partición simple de un multiconjunto de 3 elementos indistinguibles (las tareas) en 7 submulticonjuntos no ordenados que pueden ser vacíos y no unitarios (los computadores), siendo la partición ordenada (el orden de los submulticonjuntos en la partición importa para distinguir particiones, pues indica qué computadores reciben las tareas). Por ejemplo, el reparto (c_3, c_3, c_7) es la partición ordenada $\{\{\emptyset, \emptyset, \{\{\checkmark\checkmark\}\}, \emptyset, \emptyset, \emptyset, \{\{\checkmark\}\}\}\}$.

- *Interpretación de acuerdo con la modelización IV.*

  Cada reparto está representado por una descomposición simple ordenada del entero positivo 3 en 7 sumandos enteros no negativos. Por ejemplo, el reparto (c_3, c_3, c_7) (submulticonjunto $\{\{c_3, c_3, c_7\}\}$) es la siguiente descomposición simple ordenada del entero positivo 3 en 7 sumandos no negativos: $3 = 0+0+2+0+0+0+1$. La descomposición es ordenada, ya que el orden de los sumandos en la suma importa para distinguir descomposiciones; por ejemplo, la descomposición $3 = 0+0+1+0+0+0+2$ corresponde al reparto (c_3, c_7, c_7) (submulticonjunto $\{\{c_3, c_7, c_7\}\}$). ■

Ejemplo 683

Una ONG ha preparado tres tipos de obsequios para sus n personas físicas donantes. Si tiene un número suficiente de cada tipo y quiere enviar uno o más obsequios a cada una pero no quiere que ninguna reciba dos obsequios del mismo tipo, entonces, ¿de cuántas formas puede la ONG enviar los obsequios?

ⓘ Utilicemos razonadamente algún conocimiento de combinatoria para resolver esta cuestión.

[EFE 7.7.2021:8], [SEP 12.5.2022:8], [EFE 19.1.2023:8], [EFEC 29.1.2025:11] (tipo test).

Resolución.— Sea $O = \{o_{\mathrm{I}}, o_{\mathrm{II}}, o_{\mathrm{III}}\}$ el conjunto formado por los tres tipos de obsequios. Su conjunto potencia, de cardinal 2^3, es

$$\mathcal{P}(O) = \{\emptyset, \{o_{\mathrm{I}}\}, \{o_{\mathrm{II}}\}, \{o_{\mathrm{III}}\}, \{o_{\mathrm{I}}, o_{\mathrm{II}}\}, \{o_{\mathrm{I}}, o_{\mathrm{III}}\}, \{o_{\mathrm{II}}, o_{\mathrm{III}}\}, \{o_{\mathrm{I}}, o_{\mathrm{II}}, o_{\mathrm{III}}\}\}.$$

Vía 0.

Sea $\{p_0, p_1, \ldots, p_{n-1}\}$ el conjunto de las n personas físicas donantes. Subyace el *principio de la multiplicación*: el suceso S de enviar los obsequios se lleva a término en n fases que pueden considerarse sucesivas e independientes, una fase por persona física donante: S_0, S_1, ..., S_{n-1}.

Como la ONG no quiere que ninguna de sus personas físicas donantes reciba dos obsequios del mismo tipo, aunque sí al menos uno, entonces, en cada fase, se trata de una elección de subconjuntos no vacíos de obsequios, esto es, de elegir uno entre los $2^3 - 1 = 7$ subconjuntos no vacíos del conjunto O; de aquí que cada fase pueda suceder de 7 formas distintas.

Por ejemplo, haber elegido el subconjunto $\{o_{\mathrm{II}}, o_{\mathrm{III}}\}$ en la fase S_k significa que los objetos que ha recibido la persona física donante p_k son de tipo II y III.

Por tener otro punto de vista, observemos que, por ejemplo, según la modelización I —*cfr. supra* teorema 19.45 (pág. 1191 de esta edición) (cuadro n.º 0)—, cada fase corresponde a una selección simple no ordenada de $k = 1$ objetos de un total de $n = 7$ objetos distinguibles, cuyo número total es $C(7, 1) = 7$.

Como cada una de las n fases de envíos de obsequios (una por persona) puede realizarse de 7 formas distintas, entonces, por el principio de la multiplicación, el número de formas en que sucede el suceso de enviar los obsequios es

$$7 \cdot \overset{n}{\smile} \cdot 7 = 7^n.$$

Vía 1.

Un reparto es una aplicación cualquiera del conjunto $\{p_0, p_1, \ldots, p_{n-1}\}$ de las n personas en $\mathcal{P}(O) \setminus \emptyset$. El número de estas aplicaciones es $VR(7, n)$, esto es, 7^n. ■

Ejemplo 684

Una ONG recibe en su central una donación de 393 sacos idénticos de arroz. Dicha ONG decide repartirlos entre sus siete escuelas y tres hospitales asegurando que cada escuela reciba al menos 30 sacos y que cada hospital reciba al menos 60 sacos. ¿De cuántas formas puede la ONG repartir todos los sacos?

ⓘ Para resolver esta cuestión debemos: I, incluir en nuestro razonamiento alguna —a nuestra elección— de las cuatro modelizaciones combinatorias —selección, distribución, partición, descomposición aditiva—, y II, interpretar el resultado de acuerdo con cada una de las demás modelizaciones que consideremos compatibles con la situación expuesta en la cuestión en estudio.

▷ *Importante*: En cada una de las modelizaciones debemos identificar claramente cómo está representado cada reparto.

[EFO 4.6.2021:8], [EFE 19.1.2023:9], [EFO 24.5.2023:8], [EFE 3.7.2024:12] (tipo test).

Resolución.— Veamos.

I. *Inclusión en el razonamiento de alguna de las modelizaciones combinatorias estudiadas.*

0. *Discusión previa.*

Para satisfacer lo que quiere asegurar, la ONG primero reserva 30 sacos para cada escuela y 60 sacos para cada hospital, lo que hace un total de $7 \cdot 30 + 3 \cdot 60 = 210 + 180 = 390$ sacos reservados. Por tanto, los sacos que ha de repartir entre las $7 + 3 = 10$ entidades son sólo $393 - 390 = 3$, sin ninguna restricción.

Subyace en realidad el *principio de la multiplicación*.

a. *Formalización del principio de la multiplicación.*

Para poder aplicar el principio de la multiplicación debemos definir la ocurrencia del suceso S de repartir en varias fases sucesivas e independientes (cada fase de cómo se haya realizado la fase anterior, no necesariamente de qué se haya realizado). El suceso de repartir se lleva a término en estas dos fases:

$$S_0 \risingdotseq \text{reservar 30 sacos para cada escuela y 60 sacos para cada hospital;}$$
$$S_1 \risingdotseq \text{repartir los 3 sacos sobrantes entre las 10 entidades.}$$

b. *De las formas de realizar cada fase.*

La fase S_0 se hace de una única forma. La fase S_1, digamos, de N formas.

c. *Aplicación del principio de la multiplicación.*

Notando por $\#X$, tanto el número de formas en que puede suceder el suceso X como el número de formas en que puede realizarse la fase X,

$$\begin{aligned}\#S &= \#S_0 \cdot \#S_1\\ &= 1 \cdot N.\end{aligned}$$

A partir de aquí, todo consiste en hallar N.

Recordemos que una combinación con repetición de orden k de elementos de un conjunto no vacío A es un multiconjunto de elementos de A de cardinalidad k. Recordemos también que el número de combinaciones con repetición es $CR(n, k) = C(n + k - 1, k)$.

Llamemos e_0h_0 a la central, e_1, e_2, e_3, e_4, e_5, e_6, e_7, a las escuelas y h_1, h_2, h_3, a los hospitales. En la situación en estudio, cada reparto está representado por un multiconjunto de cardinalidad 3 de elementos del conjunto de entidades $A = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, h_1, h_2, h_3\}$. Por ejemplo, el reparto de dos sacos a la escuela e_5, un saco al hospital h_2 y ningún saco al resto de entidades, $/e_5, e_5, h_2/$, puede representarse por la combinación con repetición $\{\{e_5, e_5, h_2\}\}$, esto es, por dicho multiconjunto de cardinalidad 3 del conjunto A de entidades.

De este modo, el número N de formas en las que la ONG puede repartir los 3 sacos (y, por lo razonado anteriormente, el de repartir todos los sacos) es el número de combinaciones con repetición

$$\begin{aligned}CR(10, 3) &= C(10 + 3 - 1, 3)\\ &= \frac{12!}{3! \cdot 9!}\\ &= \frac{12 \cdot 11 \cdot 10}{3!}\\ &= 2 \cdot 11 \cdot 10\\ &= 220.\end{aligned}$$

Por no andar repitiéndonos, a partir de ahora, por reparto, entendemos reparto de 3 sacos iguales entre 10 entidades distintas.

Observemos finalmente que cada reparto también puede representarse por una solución entera no negativa de la ecuación $x_1 + x_2 + \ldots + x_{10} = 3$.

Tras esta presentación, centrémonos ahora en resolver la cuestión según se exige.

1. *Cálculo del recuento de acuerdo con la modelización I.*

Considerando las entidades como los objetos en el lenguaje de esta modelización, cada reparto está representado por una selección simple (muestra) con reemplazamiento [cual-

quier entidad puede recibir más de un saco y, por tanto, ser elegida más de una vez] de 3 objetos de B, un conjunto de 10 objetos distinguibles. La selección es no ordenada, pues el orden de los objetos en la muestra no importa para distinguir muestras; por ejemplo, los repartos $/e_5, e_5, h_2/$, $/e_5, h_2, e_5/$ y $/h_2, e_5, e_5/$ son idénticos: se trata del mismo submulticonjunto $\{\{e_5, e_5, h_2\}\}$. Según lo estudiado (*cfr. supra* cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—), el número total de selecciones es $CR(10, 3)$.

II. *Interpretación del resultado de acuerdo con cada una de las demás modelizaciones compatibles con la situación expuesta.*

0. Las *modelizaciones compatibles* son las cuatro estudiadas. Veamos las interpretaciones según las que restan.

1. *Interpretación de acuerdo con la modelización II.*

   Cada reparto está representado por una distribución simple de 3 objetos indistinguibles (los sacos de arroz) en 10 recipientes distinguibles (las entidades), siendo, al no existir restricción alguna, cualquiera la aplicación del multiconjunto de objetos en el conjunto de recipientes. Por ejemplo, si $\checkmark$ designa un saco indistinguible de arroz, el reparto $/e_5, e_5, h_2/$ es la distribución no ordenada $\{\checkmark \longmapsto e_5, \checkmark \longmapsto e_5, \checkmark \longmapsto h_2\}$, gráficamente

e_1	e_2	e_3	e_4	e_5	e_6	e_7	h_1	h_2	h_3
				$\checkmark\checkmark$				$\checkmark$	

   , que pudiésemos codificar en base 4 (son 3 objetos a repartir) por 0000200010. Como vemos, la distribución es no ordenada, ya que por ser los objetos indistinguibles, el orden de los mismos en cada recipiente no importa para distinguir distribuciones.

2. *Interpretación de acuerdo con la modelización III.*

   Cada reparto está representado por una partición simple de un multiconjunto de 3 elementos indistinguibles (los sacos de arroz) en 10 submulticonjuntos no ordenados que pueden ser vacíos y no unitarios (las entidades), siendo la partición ordenada (el orden de los submulticonjuntos en la partición importa para distinguir particiones, pues indica qué entidades reciben los sacos). Por ejemplo, el reparto $/e_5, e_5, h_2/$ es la partición ordenada $\langle \emptyset, \emptyset, \emptyset, \emptyset, \{\{\checkmark\checkmark\}\}, \emptyset, \emptyset, \emptyset, \{\{\checkmark\}\}, \emptyset\rangle$ (por ser ordenada, representamos la partición por una tupla de submulticonjuntos).

3. *Interpretación de acuerdo con la modelización IV.*

   Cada reparto está representado por una descomposición simple ordenada del entero positivo 3 en 10 sumandos enteros no negativos. Por ejemplo, el reparto $/e_5, e_5, h_2/$ es la siguiente descomposición simple ordenada del entero positivo 3 en 10 sumandos no negativos: $3 = 0 + 0 + 0 + 0 + 2 + 0 + 0 + 0 + 1 + 0$. La descomposición es ordenada, ya que el orden de los sumandos en la suma importa para distinguir descomposiciones; por ejemplo, la descomposición $3 = 0 + 0 + 0 + 0 + 1 + 0 + 0 + 0 + 2 + 0$ corresponde al re-

parto $/e_5, h_2, h_2/$. (Si en vez de con el signo $+$ utilizamos una representación por tuplas, a los repartos $/e_5, e_5, h_2/$ y $/e_5, h_2, h_2/$ les corresponden las tuplas $\langle 0,0,0,0,2,0,0,0,1,0\rangle$ y $\langle 0,0,0,0,1,0,0,0,2,0\rangle$). ■

Observación 19.3.8.— Recordemos de nuevo que si A es el conjunto subyacente del multiconjunto $\{\{a_1, \overset{k}{\ldots}, a_1, a_2, \overset{k}{\ldots}, a_2, \ldots, a_n, \overset{k}{\ldots}, a_n\}\}$, una combinación con repetición de orden k de elementos de A es una aplicación de A en $\{0,1,\ldots,k\}$ tal que a cada elemento a_i de $A = \{a_1, a_2, \ldots, a_n\}$ le asocia el número de veces (entre 0 y k) que aparece repetido a_i en un submulticonjunto del multiconjunto, sujeta dicha aplicación a la condición de que la suma de tales números sea k. Observemos que tal aplicación define precisamente al submulticonjunto con esta característica.

En la situación en estudio en el ejemplo anterior, cada reparto está representado por una aplicación del conjunto de entidades $A = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, h_1, h_2, h_3\}$ en $\{0,1,2,3\}$ tal que a cada entidad le asocia el número de sacos que le corresponden sujeta a la condición de que la suma de tales números es 3. Por ejemplo, el reparto de dos sacos a la escuela e_5, un saco al hospital h_2 y ningún saco al resto de entidades, $/e_5, e_5, h_2/$, puede representarse por la combinación con repetición $\{\{e_5, e_5, h_2\}\}$, esto es, por dicho submulticonjunto del multiconjunto $\{\{e_1, e_1, e_1, e_2, e_2, e_2, \ldots, e_7, e_7, e_7, h_1, h_1, h_1, \ldots, h_3, h_3, h_3\}\}$, es decir, por la aplicación $\{e_1 \longmapsto 0, e_2 \longmapsto 0, e_3 \longmapsto 0, e_4 \longmapsto 0, e_5 \longmapsto 2, e_6 \longmapsto 0, e_7 \longmapsto 0, h_1 \longmapsto 0, h_2 \longmapsto 1, h_3 \longmapsto 0\}$.

Observación 19.3.9.— Calcular por separado el número de repartos a hospitales y a escuelas para después agregar los resultados no es correcto, ya que los repartos comunes, esto es, en los que participen escuelas y hospitales (por ejemplo, $/e_1, e_6, h_2/$), no entrarían en tal recuento.

Ejemplo 685

Se dispone de dos listas A y B, de n personas cada una. ¿De cuántas formas pueden emparejarse todas las personas de la lista A con todas las de B?

ⓘ Para resolver esta cuestión debemos: I, incluir en nuestro razonamiento alguna —a nuestra elección— de las cuatro modelizaciones combinatorias —selección, distribución, partición, descomposición aditiva—, y II, interpretar el resultado de acuerdo con cada una de las demás modelizaciones que consideremos compatibles con la situación expuesta en la cuestión en estudio.

▷ *Importante*: En cada una de las modelizaciones debemos identificar claramente cómo está representado cada emparejamiento.

[EFO 4.6.2021:7], [EFE 22.6.2022:9], [EFE 28.6.2023:8].

Resolución.— Representando cada persona de la lista A por su posición en ella, cada emparejamiento es una aplicación inyectiva del conjunto $\{0,1,\ldots,n-1\}$ en B, esto es, una variación de n elementos de los n elementos del conjunto B. Por tanto, el número total de emparejamientos es el número de variaciones $V(n,n) = n^{\underline{n}} = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-n+1) = n!$ (al tener A y B el

mismo cardinal n, un emparejamiento es en realidad una aplicación biyectiva y de ahí que el número sea el de permutaciones de n elementos).

Esto ha sido por definición de variación. En cada una de ellas, la posición de la persona de la lista B indica la persona de la lista A con la que está emparejada; por ejemplo, si $n = 2$ y las listas son $A \leftrightharpoons a_0 a_1$ y $B \leftrightharpoons b_0 b_1$, entonces la variación $\langle b_0, b_1 \rangle$ representa el emparejamiento $\{a_0 \longleftrightarrow b_0, a_1 \longleftrightarrow b_1\}$, mientras que la variación $\langle b_1, b_0 \rangle$ representa el emparejamiento $\{a_0 \longleftrightarrow b_1, a_1 \longleftrightarrow b_0\}$.

Tras esta presentación, centrémonos ahora en resolver la cuestión según se exige.

I. *Cálculo del recuento de acuerdo con la modelización I.*

Considerando las personas como los objetos en el lenguaje de esta modelización, cada emparejamiento está representado por una selección simple (muestra) ordenada (como hemos visto, el orden de los objetos en la muestra importa para distinguir muestras) sin reemplazamiento de n objetos de B, un conjunto de n objetos distinguibles (sin reemplazamiento porque $\langle b_i, b_i \rangle$ significaría que la persona b_i se ha emparejado con dos personas diferentes de la lista A).

De este modo, en el ejemplo anterior, siendo $n = 2$ y las listas $A \leftrightharpoons a_0 a_1$ y $B \leftrightharpoons b_0 b_1$, entonces la muestra $\langle b_0, b_1 \rangle$ representa el emparejamiento $\{a_0 \longleftrightarrow b_0, a_1 \longleftrightarrow b_1\}$, mientras que la muestra $\langle b_1, b_0 \rangle$ representa el emparejamiento $\{a_0 \longleftrightarrow b_1, a_1 \longleftrightarrow b_0\}$.

Así, según lo estudiado (*cfr. supra* cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—), el número total de selecciones es $V(n, n) = n^{\underline{n}} = n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot (n-n+1) = n!$.

II. *Interpretación del resultado de acuerdo con cada una de las demás modelizaciones compatibles con la situación expuesta.*

0. *Interpretación de acuerdo con la modelización II.*

Cada emparejamiento está representado por una distribución simple de n «objetos» distinguibles (personas de A) en n «recipientes» distinguibles (personas de B), siendo biyectiva la aplicación del conjunto de objetos en el de recipientes (en efecto, es inyectiva porque ninguna persona de B está emparejada con más de una de A y es sobreyectiva porque cada persona de B está emparejada con al menos una persona de A) y siendo la distribución no ordenada, pues el orden de los objetos en cada recipiente no importa para distinguir distribuciones, ya que únicamente hay un objeto en cada recipiente.

De este modo, en el ejemplo anterior, siendo $n = 2$ y las listas $A \leftrightharpoons a_0 a_1$ y $B \leftrightharpoons b_0 b_1$, entonces la distribución $\{a_0 \longmapsto b_0, a_1 \longmapsto b_1\}$ representa el emparejamiento $\{a_0 \longleftrightarrow b_0, a_1 \longleftrightarrow b_1\}$, mientras que la distribución $\{a_0 \longmapsto b_1, a_1 \longmapsto b_0\}$ representa el emparejamiento $\{a_0 \longleftrightarrow b_1, a_1 \longleftrightarrow b_0\}$.

Observación.— En vez de haber destacado la biyectividad de la aplicación, pudiésemos haber destacado su inyectividad o su sobreyectividad, pues en ambos casos, ser aplicación y

tener el mismo cardinal, obliga a la biyectividad. Recordando lo estudiado (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—), somos capaces de demostrar que si hubiésemos destacado su inyectividad, el número total de distribuciones es $V(n,n)$, esto es, $n!$, y caso de haber destacado su sobreyectividad, el número total de distribuciones es $P(n) \cdot S(n,n) = n! \cdot 1 = n!$.

1. *Interpretación de acuerdo con la modelización III.*

   Cada emparejamiento está representado por una partición simple ordenada de un conjunto de n elementos distinguibles (personas de B) en n subconjuntos ordenados o no y unitarios (son unitarios porque se emparejan «simultáneamente» sólo con uno de B; además, no pueden ser vacíos porque no queda ninguna persona de B sin emparejar y el cardinal de B es el número de subconjuntos), siendo la partición ordenada (el orden de los subconjuntos en la partición importa para distinguir particiones).

   De este modo, en el ejemplo anterior, siendo $n = 2$ y las listas $A \leftrightharpoons a_0a_1$ y $B \leftrightharpoons b_0b_1$, entonces la partición ordenada de subconjuntos $\langle\{b_0\},\{b_1\}\rangle$ o de subconjuntos ordenados $\langle\langle b_0\rangle,\langle b_1\rangle\rangle$ representa el emparejamiento $\{a_0 \longleftrightarrow b_0, a_1 \longleftrightarrow b_1\}$, mientras que la partición ordenada de subconjuntos $\langle\{b_1\},\{b_0\}\rangle$ o de subconjuntos ordenados $\langle\langle b_1\rangle,\langle b_0\rangle\rangle$ representa el emparejamiento $\{a_0 \longleftrightarrow b_1, a_1 \longleftrightarrow b_0\}$.

2. *Interpretación de acuerdo con la modelización IV.*

   Las *modelizaciones compatibles* son la I, II y III. La IV no lo es porque al representar un entero positivo k como la suma de k unos, estos unos, indistinguibles, son los correspondientes a los objetos, que, por tanto, deberían ser indistinguibles, pero en la situación en estudio, el lugar de estos objetos lo ocupan personas, que son distinguibles (*cfr. supra* cuadro n.º 7 —teorema 19.58 (pág. 1212 de esta edición)—). ■

Ejemplo 686

Antes de un examen, una profesora repartió una lista con doce posibles cuestiones. El examen constaba de cuatro cuestiones de esas doce. ¿Cuántos posibles exámenes distintos existen?, esto es, ¿cuántas posibilidades existen de elegir las cuatro cuestiones entre las doce?

[EFO 1.6.2017:6a2], [EFO 20.5.2022:9], [SEL 10:5a2]. *Cfr.* FERRANDO y GREGORY [156]: ejercicio 5.2 (pág. 197).

Resolución.— Aunque no se pide, tratemos de reescribir cada elección de cuatro cuestiones entre las doce en las cuatro modelizaciones.

Cada elección de cuatro cuestiones entre las doce posibles es:

- según la modelización I, una muestra no ordenada —el orden de las cuestiones en el examen da igual— de $k = 4$ objetos —las cuatro cuestiones definitivas del examen— procedente de un muestreo sin reemplazamiento —no hay cuestiones repetidas en un examen— de $n = 12$ tipos distinguibles de objetos; por ejemplo, la elección de las preguntas 3, 5, 7 y 11 es la muestra no ordenada $\{3, 5, 7, 11\}$; así, existen $C(12, 4) = 495$ posibilidades de elegir las cuatro cuestiones entre las doce (*cfr. supra* cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—);

- según la modelización II, una distribución no ordenada (el orden de los objetos dentro de los recipientes es irrelevante, pues como mucho hay un objeto en cada recipiente) de $k = 4$ objetos indistinguibles (marcas de elección) en $n = 12$ recipientes (las doce cuestiones) distinguibles no pudiendo ningún recipiente contener más de un objeto (la aplicación subyacente $f : O \longrightarrow R$ de objetos en recipientes es inyectiva —una cuestión no puede ser doblemente elegida, pues significaría una misma pregunta repetida en un mismo examen—); por ejemplo, la elección de las preguntas 3, 5, 7 y 11 es la distribución no ordenada $\{\checkmark \longmapsto 3, \checkmark \longmapsto 5, \checkmark \longmapsto 7, \checkmark \longmapsto 11\}$, gráficamente

1	2	3	4	5	6	7	8	9	10	11	12
		✓		✓		✓				✓	

, que pudiésemos codificar como 001010100010; así, existen $C(12, 4) = 495$ posibilidades de elegir las cuatro cuestiones entre las doce (*cfr. supra* cuadro n.º 2 —teorema 19.47 (pág. 1198 de esta edición)—).

- según la modelización III, una partición ordenada de un multiconjunto de cuatro elementos indistinguibles (marcas de elección) en doce submulticonjuntos no ordenados (las doce cuestiones) entre los que puede haberlos vacíos y unitarios (una cuestión no puede ser doblemente elegida, pues significaría una misma pregunta repetida en un mismo examen); por ejemplo, la elección de las preguntas 3, 5, 7 y 11 es la partición ordenada $\{\{\emptyset, \emptyset, \{\{\checkmark\}\}, \emptyset, \{\{\checkmark\}\}, \emptyset, \{\{\checkmark\}\}, \emptyset, \emptyset, \emptyset, \{\{\checkmark\}\}, \emptyset\}\}$ del multiconjunto $\{\{\checkmark, \checkmark, \checkmark, \checkmark\}\}$; así, existen $C(12, 4) = 495$ posibilidades de elegir las cuatro cuestiones entre las doce —*cfr. supra* cuadro n.º 5 —teorema 19.52 (pág. 1205 de esta edición)—).

- según la modelización IV, una descomposición ordenada (el orden es la forma de identificar las cuestiones) del número entero positivo 4 en doce sumandos enteros no negativos; por ejemplo, la elección de las preguntas 3, 5, 7 y 11 es la descomposición ordenada $12 = 0 + 0 + 1 + 0 + 1 + 0 + 1 + 0 + 0 + 0 + 1 + 0$; así, existen C(12,4) = 495 posibilidades de elegir las cuatro cuestiones entre las doce (*cfr. supra* cuadro n.º 6 —teorema 19.57 (pág. 1210 de esta edición)—).

  Solución.— Existen 495 posibilidades de elegir las cuatro cuestiones entre las doce. ■

Observación 19.3.10.— Sobre la modelización I (aunque no es el caso que nos ha ocupado en el ejemplo anterior): imaginemos por un momento (insistimos, no ha sido el caso) que el orden de las preguntas importase, esto es, que, por ejemplo, el examen $/3, 5, 7, 11/$ fuese distinto del examen $/5, 3, 7, 11/$, entonces se trataría de una muestra ordenada de $k = 4$ objetos [las cuatro cuestiones definitivas del examen] procedente de un muestreo sin reemplazamiento [no hay cuestiones repetidas en un examen] de $n = 12$ tipos distinguibles de objetos; entonces, por ejemplo, la elección de

las preguntas 3, 5, 7 y 11, en las dos selecciones ordenadas anteriores de ejemplo, podría codificarse, como muestra ordenada $\langle 3, 5, 7, 11\rangle$, indicando el orden de cada elemento en la selección, esto es, como 001020300040 y como muestra ordenada $\langle 5, 3, 7, 11\rangle$, indicando el orden de cada elemento en la selección, esto es, como 002010300040; como vemos, el número total de selecciones sería el número de variaciones de cuatro elementos de un conjunto de doce, es decir, $V(12, 4) = 12 \cdot 11 \cdot 10 \cdot 9 = 11880$ —*cfr. supra* cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—); recordemos una vez más, esta situación no es la analizada en el ejemplo anterior.

Ejemplo 687

En el examen del ejemplo anterior, una persona sólo tuvo tiempo de preparar siete de las doce cuestiones, ¿cuántas posibilidades le favorecieron?

[EFO 1.6.2017:6a1], [SEL 10:5a1]. *Cfr.* Ferrando y Gregory [156]: ejercicio 5.2 (pág. 197).

Resolución.— Como no dice nada sobre la calificación, suponemos que las cuatro preguntas se califican por igual, entonces, que un posible examen le favorezca significa que mínimo ha de haber preparado 2 de las 4 preguntas, habrá tres casos que le favorezcan:

0.°, que el examen contenga 2 de las preguntas preparadas;

1.°, que el examen contenga 3 de las preguntas preparadas, y

2.°, que todas las preguntas del examen sean de las que había preparado.

Usemos la modelización I (*cfr. supra* cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—) (las preguntas son los objetos):

- caso 0.º: pensando en una muestra no ordenada (el orden de los objetos no importa para distinguir dos muestras; en nuestro caso, preocuparnos por las preguntas A y B es lo mismo que preocuparnos por las preguntas B y A) de 2 objetos de un total de 7 objetos distinguibles (las preguntas preparadas), procedente de un muestreo sin reemplazamiento (en un examen no puede haber preguntas repetidas), tendríamos que el número total de selecciones es $C(7, 2)$, ¿y ya está?, ¿es $C(7, 2)$ el número total de selecciones correspondientes a este caso 0.º? Pues no, faltan las otras 2 preguntas; observemos que el objetivo final al dividir en los tres casos es aplicar el principio de la adición, y para poder aplicar este principio, los conjuntos deben ser disjuntos dos a dos, luego en el caso 0.º decimos en realidad: «que el examen contenga exactamente 2 de las preguntas preparadas», esto es, «2 de las preguntas de entre las 7 preparadas y 2 de las preguntas de entre las 5 no preparadas»; esto corresponde al principio de la multiplicación [¡esto requiere justificación! ✍] y, entonces, el número total de selecciones correspondientes al caso 0.º es $C(7, 2) \cdot C(5, 2)$;

- caso 1.º: «que el examen contenga exactamente 3 de las preguntas preparadas», esto es, «3 de las preguntas de entre las 7 preparadas y 1 de las preguntas de entre las 5 no preparadas» y, por un razonamiento similar, el número total de selecciones correspondientes al caso 2 es $C(7,3)\cdot C(5,1)$;
- caso 2.º: «que el examen contenga exactamente 4 de las preguntas preparadas», esto es, «4 de las preguntas de entre las 7 preparadas y 0 de las preguntas de entre las 5 no preparadas» y, por un razonamiento similar, el número total de selecciones correspondientes al caso 2.º es $C(7,4)\cdot C(5,0)$.

Así, aplicando ahora el principio de la adición [¡esto requiere justificación! ✍], $C(7,2)\cdot C(5,2)+C(7,3)\cdot C(5,1)+C(7,4)\cdot C(5,0)=420$. ■

Actividad 19.21

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición y el principio de la multiplicación, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Ejemplo 688

En el examen del ejemplo anterior, si en opinión de la profesora había dos cuestiones que no podían aparecer en el mismo examen, ¿cuál fue en realidad el total de posibilidades?

[EFO 1.6.2017:6b], [SEL 10:5b]. *Cfr.* FERRANDO y GREGORY [156]: ejercicio 5.1 (pág. 197).

Resolución.— Sean a y b las cuestiones que no pueden aparecer juntas en el mismo examen. Pero, ¿qué significa que las cuestiones a y b no aparezcan juntas en el mismo examen? Se trata justo de los tres casos correspondientes a la negación de la conjunción a y b. Puede suceder:

0.°, ni a ni b aparecen,

1.°, a aparece y b no aparece,

2.°, b aparece y a no aparece.

Recordemos que cuando resolvimos el ejemplo 686 (pág. 1228 de esta edición), lo hicimos según las cuatro modelizaciones. Cualquiera de estos tres casos se puede resolver de una manera similar.

Por ejemplo:

- caso 0.º: resolvámoslo por la modelización II; excluyendo a y b, quedan 10 cuestiones; cada elección de 4 de entre estas 10 es una distribución no ordenada (el orden de los objetos dentro de los recipientes es irrelevante) de 4 objetos indistinguibles (marcas de elección) en 10 re-

cipientes distinguibles (las 10 cuestiones) no pudiendo ningún recipiente contener más de un objeto (la aplicación subyacente $f : O \longrightarrow R$ de objetos en recipientes es inyectiva) (una cuestión no puede ser elegida más de una vez, pues significaría una misma pregunta repetida en un mismo examen) (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—); por ejemplo, la elección de las preguntas 2, 3, 5 y 7 es la distribución no ordenada gráficamente

c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}
	✓	✓		✓		✓			

; así, existen $C(10, 4) = 210$ posibilidades de elegir 4 cuestiones entre las 10; esto significa que es posible formar $C(10, 4) = 210$ exámenes que no incluyen ni la cuestión a ni la b;

- caso 1.º: resolvámoslo por la modelización III; a es una cuestión fija del examen, así que no tiene nada que ver con el recuento, es como si el examen consistiera de sólo tres cuestiones; por otro lado, b no puede participar en el recuento; por tanto, se trata de que tenemos que elegir 3 cuestiones entre las 10 posibles; cada elección de 3 cuestiones entre las 10 posibles es una partición ordenada de un multiconjunto de 3 elementos indistinguibles (marcas de elección) en 10 submulticonjuntos no ordenados (las 10 cuestiones) entre los que puede haberlos vacíos y unitarios (una cuestión no puede ser elegida más de una vez, pues significaría una misma pregunta repetida en un mismo examen) (*cfr. supra* cuadro n.º 4.a —teorema 19.52 (pág. 1205 de esta edición)—); por ejemplo, la elección de las preguntas 2, 3 y 5 es la partición ordenada $\{\{\emptyset, \{\{\checkmark\}\}, \{\{\checkmark\}\}, \emptyset, \{\{\checkmark\}\}, \emptyset, \emptyset, \emptyset, \emptyset, \emptyset\}\}$ del multiconjunto $\{\{\checkmark, \checkmark, \checkmark\}\}$; así, existen $C(10, 3) = 120$ posibilidades de elegir 3 cuestiones entre las 10; esto significa que es posible formar $C(10, 3) = 120$ exámenes que incluyen la cuestión a y no incluyen la cuestión b.

- 2.º: resolvámoslo por la modelización IV; cada elección de tres cuestiones entre las diez posibles es una descomposición ordenada (el orden es la forma de identificar las cuestiones) del número entero positivo 3 en 10 sumandos enteros no negativos; por ejemplo, la elección de las preguntas 2, 3 y 5 es la descomposición ordenada $3 = 0+1+1+0+1+0+0+0+0+0$; esto significa que es posible formar $C(10, 3) = 120$ exámenes que incluyen la cuestión b y no incluyen la cuestión a.

Ahora, tenemos que definir un número finito de sucesos, incompatibles dos a dos, para poder aplicar el principio de la adición, con el fin de agregar todo; concrentamente, tres sucesos:

- S_0: «ni la cuestión a ni la b aparecen en el examen», que ocurre de $C(10, 4)$ diferentes maneras;

- S_2: «la cuestión a aparece en el examen pero la cuestión b no», que ocurre de $C(10, 3)$ diferentes maneras;

- S_3: «la cuestión b aparece en el examen pero la cuestión a no»,que ocurre de $C(10, 3)$ diferentes maneras.

Parece claro que S_1, S_2, S_3 son sucesos incompatibles dos a dos, por tanto, puede aplicarse el principio de la adición y entonces:

$$\begin{aligned} |S_1 \cup S_2 \cup S_3| &= |S_1| + |S_2| + |S_3| \\ &= C(10,4) + C(10,3) + C(10,3) \\ &= 210 + 120 + 120 \\ &= 450. \end{aligned}$$



Observación 19.3.11.— En la formulación del principio de la adición en términos de conjuntos, éstos serían:

$$\begin{aligned} S_1 &= \{x : \text{ ni la cuestión } a \text{ ni la } b \text{ aparecen en } x\}, \\ S_2 &= \{x : \text{ la cuestión } a \text{ aparece en } x \text{ pero la cuestión } b \text{ no}\}, \\ S_3 &= \{x : \text{ la cuestión } b \text{ aparece en } x \text{ pero la cuestión } a \text{ no}\}. \end{aligned}$$

§ 19.4 Grafos en combinatoria

Veamos un ejemplo de demostración combinatoria con grafos.

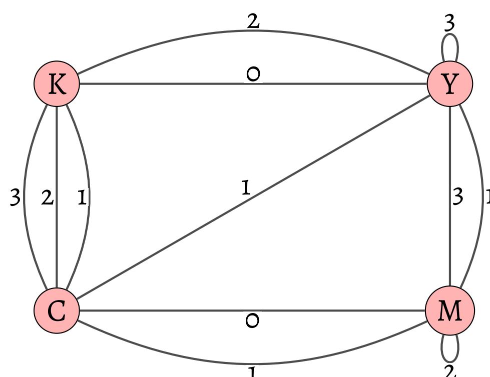
Ejemplo 689

Sean cuatro equipos (E_0, E_1, E_2 y E_3) de seis personas cada uno, expertas en cuatro conocimientos (C, M, Y y K); notando por su conocimiento las personas, estos equipos son los multiconjuntos: $E_0 = \{\{C, C, M, Y, Y, K\}\}$, $E_1 = \{\{C, C, M, M, Y, K\}\}$, $E_2 = \{\{C, M, M, Y, K, K\}\}$ y $E_3 = \{\{C, M, Y, Y, Y, K\}\}$. Sean cuatro proyectos (P_0, P_1, P_2 y P_3), cada uno involucrando necesariamente dichos cuatro conocimientos, pero cuyas metas son opuestas dos a dos —digamos, por ejemplo, que la meta de P_0 es opuesta a la de P_1 y la de P_2 es opuesta a la de P_3—. Debemos distribuir esta fuerza de trabajo en estos cuatro proyectos atendiendo a dos requisitos, por una parte, debemos asignar a los proyectos las personas de cada equipo por oposición de metas —esto es, siguiendo el ejemplo, si una trabaja, digamos, en P_0, la otra trabaja en P_1—, concretamente están en oposición:

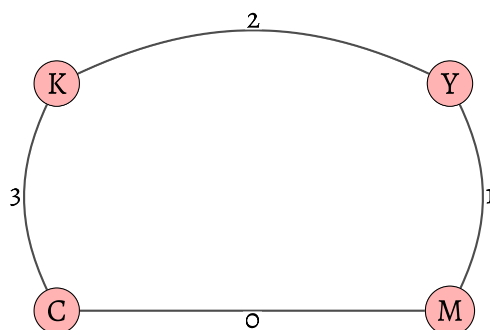
- en E_0, una C con la M, la otra C con una Y, y la otra Y con la K;
- en E_1, una C con la K, la otra C con una M, y la otra M con la Y;
- en E_2, una K con la Y, la otra K con la C, y las dos M entre sí;
- en E_3, una Y con la M, la C con la K, y las otras dos Y entre sí;

y, por otra, no deben repetirse los conocimientos en ningún proyecto.

Resolución.— Construimos un grafo no dirigido con los vértices los conocimientos, conectando éstos según la oposición prescrita para las personas e indicando el número en el eje el equipo en el que se da dicha oposición.



Para hallar una distribución, debemos encontrar un ciclo de cuatro ejes (uno por equipo), de manera que cada conocimiento aparezca sólo una vez.

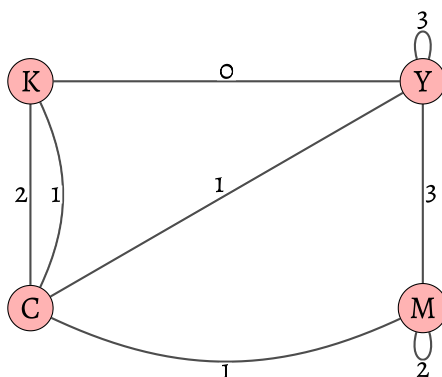


La lectura de este ciclo nos proporciona pares de conocimientos en oposición en cada equipo (C y M son opuestos en E_0, M e Y lo son en E_1, Y y K lo son en E_2, y K y C lo son en E_3), por lo que basta asignar las primeras componentes a un proyecto, digamos P_0, y las segundas al otro en oposición, P_1:

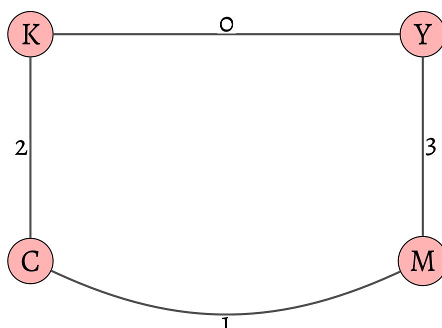
$$(P_0)^{\langle E_0,E_1,E_2,E_3\rangle}_{\langle C,M,Y,K\rangle} \qquad \text{y} \qquad (P_1)^{\langle E_0,E_1,E_2,E_3\rangle}_{\langle M,Y,K,C\rangle},$$

esto es, en P_0, los conocimientos aportados por los equipos E_0, E_1, E_2 y E_3 son C, M, Y y K, respectivamente, y en P_1, los conocimientos aportados por los equipos E_0, E_1, E_2 y E_3 son M, Y, K y C, respectivamente.

Tras suprimir el ciclo encontrado queda el siguiente grafo.



En este grafo debemos repetir el proceso, esto es, tenemos que encontrar un ciclo de cuatro ejes en el que cada conocimiento aparezca sólo una vez.



La lectura de este ciclo nos proporciona pares de conocimientos en oposición en cada equipo (Y y K son opuestos en E_0, C e M lo son en E_1, K y C lo son en E_2, y M e Y lo son en E_3), por lo que basta asignar las primeras componentes a un proyecto, digamos P_2 y las segundas al otro en oposición, P_3:

$$(P_2)^{\langle E_0,E_1,E_2,E_3\rangle}_{\langle Y,C,K,M\rangle} \qquad \text{y} \qquad (P_3)^{\langle E_0,E_1,E_2,E_3\rangle}_{\langle K,M,C,Y\rangle},$$

esto es, en P_2, los conocimientos aportados por los equipos E_0, E_1, E_2 y E_3 son Y, C, K y M, respectivamente, y en P_3, los conocimientos aportados por los equipos E_0, E_1, E_2 y E_3 son K, M, C e Y, respectivamente. ■

§ 19.5 Un ejemplo de modelización no simple

La permutación con repetición, que si es de orden $k_1, k_2, \ldots, k_n$, su número es $PR_{k_1,k_2,\ldots,k_n}$. Siguen las interpretaciones de una permutación con repetición como selección no simple, como distribución no simple y como partición no simple.

Como selección no simple

Es una selección ordenada, con reemplazamiento, de $k_1 + k_2 + \cdots + k_n$ objetos de n objetos distinguibles en la que se exige que el objeto i sea elegido k_i veces.

Como distribución no simple

Es una distribución no ordenada de $k_1 + k_2 + \cdots + k_n$ objetos distinguibles en n recipientes distinguibles en la que se exige que el recipiente i contenga k_i objetos.

Como partición no simple

Es una partición ordenada de un conjunto de $k_1 + k_2 + \cdots + k_n$ elementos (distinguibles) en n subconjuntos ordenados en la que se exige que el subconjunto i contenga k_i elementos.

Ejemplo 690

La cuadrícula de Manhattan consta de doce avenidas recorriendo de norte a sur la isla (Broadway es la excepción, pues la recorre en diagonal, y no hablamos de ella) —la primera avenida (1st *Avenue*) está en el extremo este de Manhattan, junto al *East River*, y la última, la doce (12th *Avenue*) está en el extremo oeste, junto al río Hudson—, cortadas en ángulos rectos por más de 210 calles, que recorren la isla de este a oeste. La numeración de las calles es de sur a norte, esto es, la primera (1st *St*) está en el sur de Manhattan —así, si al recorrer una avenida los números de las calles que cruzan crecen, es que caminamos hacia el norte—. La cuestión es, ¿cuántos caminos de longitud mínima pueden seguirse para ir del cruce de la 3.ª Avenida con la calle 23 (3rd *Avenue* 23rd *St*) hasta el cruce de la 6.ª Avenida con la calle 17 (6th *Avenue* 17th *St*)?

[EFO 20.5.2022:8].

Resolución.— Notemos por ← cada recorrido de una manzana de este a oeste (arista horizontal) y por ↓ cada recorrido de una manzana de norte a sur (arista vertical).

Para ir del cruce de la 3.ª Avenida con la calle 23 hasta el cruce de la 6.ª Avenida con la calle 17 por un camino de longitud mínima, hay que recorrer tres manzanas de este a oeste (6.ª ← 5.ª ← 4.ª ← 3.ª) y seis manzanas de norte a sur, de la calle 23 a la 17, un total de nueve manzanas o etapas (recorridos de una manzana) que pudiésemos numerar, de la 1.ª a la 9.ª. De hecho, cualquiera de los caminos de longitud mínima que nos interesan está compuesto de nueve recorridos de una manzana, tres de la forma ← y seis de la forma ↓. Un ejemplo, en la figura 19.0 (pág. 1237 de esta edición).

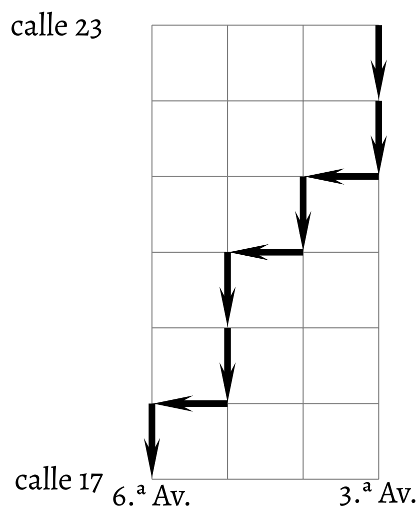


Figura 19.0.— Ejemplo de camino de longitud mínima desde el cruce de la 3.ª avenida con la calle 23 hasta el cruce de la 6.ª avenida con la calle 17.

En fin, que cada camino de longitud mínima corresponde a una aplicación sobreyectiva de un conjunto de nueve elementos (los nueve recorridos de una manzana), digamos $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, en el conjunto de símbolos $B = \{\leftarrow, \downarrow\}$, de tal forma que tres elementos de A tienen la misma imagen $\leftarrow$ en B y seis elementos de A tienen la misma imagen $\downarrow$ en B; así, cada camino de longitud mínima es una permutación con repetición de orden $(3, 6)$; entonces, el número de posibles camino de longitud mínima es el número de permutaciones con repetición; por tanto, hay $PR(3, 6) = (3 + 6)!/(3! \cdot 6!) = 84$ caminos de longitud mínima para ir del cruce de la 3.ª Avenida con la calle 23 hasta el cruce de la 6.ª Avenida con la calle 17.

Solución.— Existen 84 caminos de longitud mínima para ir del cruce de la 3.ª Avenida con la calle 23 hasta el cruce de la 6.ª Avenida con la calle 17. ■

Observación 19.5.0.— Éste ha sido un problema de recuento del número de caminos de longitud mínima (orientados) entre dos vértices de un grafo no dirigido.

Observación 19.5.1.— El resultado coincide con el número de combinaciones $C(9, 3)$ y $C(9, 6)$. Es un buen ejercicio tratar de ver cada camino de longitud mínima como una combinación; de paso, tratar también de verlo como una selección no ordenada sin reemplazamiento de tres (o seis) objetos de un total de nueve objetos distinguibles (*cfr. supra* cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—).

Ejemplo 691

Realicemos una demostración combinatoria (sin usar los conceptos, ni de número factorial ni de número factorial descendente ni de número factorial ascendente) de

$$C(n, k) = C(n, n - k).$$

[Cubit 141].

Resolución.— Una combinación de k elementos de un conjunto de n elementos puede interpretarse según la modelización I como una selección no ordenada de k objetos de un total de n objetos distinguibles sin reposición. Observemos que al elegir explícitamente estos k objetos, elegimos implícitamente los otros $n - k$ objetos, por lo que estamos ante una combinación de $n - k$ elementos de un conjunto de n elementos. ■

Ejemplo 692

Realicemos una demostración combinatoria (sin usar los conceptos, ni de número factorial ni de número factorial descendente ni de número factorial ascendente) de la identidad de Pascal:

$$C(n + 1, k) = C(n, k) + C(n, k - 1).$$

Resolución.— Una combinación de k elementos de un conjunto de $n + 1$ elementos puede interpretarse según la modelización I como una selección no ordenada de k objetos de un total de $n+1$ objetos distinguibles sin reposición. Observemos que al elegir explícitamente estos k objetos, bien excluimos uno de ellos, llamémosle O, en cuyo caso seleccionamos k de los restantes n, bien seleccionamos O, seleccionando entonces los restantes $k - 1$ (para así haber seleccionado un total de k) de los restantes n objetos. ■

Ejemplo 693

Sea la malla tridimensional cuadriculada con vértices de coordenadas enteras. Llamamos arista al segmento que une dos vértices consecutivos. Definimos un camino entre dos vértices como el conjunto de aristas que un punto imaginario ha de recorrer para llegar de un vértice a otro. ¿Cuál es el número total de caminos entre dos vértices cualesquiera?

Resolución.— Siendo los vértices (x_1, y_1, z_1) y (x_2, y_2, z_2), deben recorrerse $x_2 - x_1$ aristas en la dirección del eje OX, $y_2 - y_1$ en la de OY y $z_2 - z_1$ en la de OZ; un total de $(x_2 - x_1) + (y_2 - y_1) + (z_2 - z_1)$ aristas; así, el total de caminos viene dado por $PR_{x_2 - x_1, y_2 - y_1, z_2 - z_1}$. ■

§ 19.6 Muestra de más ejemplos

Ejemplo 694

Un restaurante tiene una oferta de siete menús, ofreciendo cada día uno de ellos como menú del día.

0. Un menú semanal variado es una colección de siete menús diarios todos diferentes.
   a. ¿Cuántas distribuciones de menús semanales variados son posibles?
   b. ¿Y si la oferta del restaurante fuese de ocho menús en vez de siete?
1. Un día festivo determinado, el restaurante ofrece no sólo uno sino los siete menús como menús del día. ¿De cuántas formas puede pedir comida un grupo de cuatro personas si cada una quiere menú?

[EFE 29.6.2018:6], [EFE 29.1.2025:11] (tipo test), [EFE 29.1.2025:12] (tipo test).

Resolución.—

0. a. Son siete objetos distinguibles —los días de la semana— a distribuir en siete recipientes distinguibles —los menús diarios—; mínimo y máximo un objeto por recipiente —un día por menú, ya que en un menú semanal variado todos los menús diarios son diferentes—, por lo que la aplicación es biyectiva; al ser un único objeto en cada recipiente, el orden de los objetos dentro de cada recipiente no importa —distribución no ordenada—. Entonces (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—),

$$\begin{aligned} P(7) &= 7! \\ &= 5040. \end{aligned}$$

   b. Son siete objetos distinguibles —los días de la semana— a distribuir en ocho recipientes distinguibles —los menús diarios—; máximo un objeto por recipiente —un día por menú, ya que en un menú semanal variado todos los menús diarios son diferentes—, por lo que la aplicación es inyectiva —no puede ser sobreyectiva porque hay más recipientes que objetos—; al ser un máximo de un objeto por recipiente, el orden de los objetos dentro de cada recipiente no importa —distribución no ordenada—. Entonces (*cfr. supra* cuadro n.º

2.a —teorema 19.47 (pág. 1198 de esta edición)—),

$$\begin{aligned} V(8,7) &= 8^{[7]} \\ &= \frac{8!}{1!} \\ &= 8 \cdot 7! \\ &= 8 \cdot 5040 \\ &= 40320. \end{aligned}$$

1. Son cuatro objetos indistinguibles —las personas, indistinguibles porque sólo interesa cuántas eligen cada menú, no quiénes— a distribuir en siete recipientes distinguibles —los menús; no existe restricción para la aplicación del multiconjunto de objetos en el conjunto de recipientes; por ser los objetos indistinguibles, su orden dentro de cada recipiente no importa —distribución no ordenada—. Entonces (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—),

$$\begin{aligned} CR(7,4) &= \binom{7+4-1}{4} \\ &= \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6!}{4 \cdot 3 \cdot 2 \cdot 6!} \\ &= 210. \end{aligned}$$

Recordemos que $CR(n,k) = \binom{n+k-1}{k}$. ■

Ejemplo 695

¿Cuál es el valor máximo posible del número de filas n de una matriz binaria M de orden $n \times 10$, sabiendo que M no tiene dos filas iguales?

[EPF 14.5.2019:7].

Resolución.— Destaquemos dos vías.

Vía 0.

El número máximo de filas de M es el número de formas de distribuir 10 objetos distinguibles —los elementos de la matriz como parámetros formales— en 2 recipientes distinguibles —los símbolos 0 y 1—, sin importar el orden de colocación de los objetos dentro de los recipientes. Por otro lado, la aplicación subyacente a una fila cualquiera j, de objetos en recipientes, $f_j : \{a_{j1}, a_{j10}\} \longrightarrow \{0,1\}$ no está sujeta a ninguna restricción: elementos distintos de una misma fila pueden tener el mismo valor por lo que no se exige inyectividad y puede que todos los elementos de una misma fila tengan el mismo valor. De acuerdo con los teoremas conocidos en el ámbito de la modelización como problema de distribución/ocupación, se tiene que dicho número máximo es $VR_{2,10} = 2^{10}$. □

Vía 1.

Contar las filas de la matriz por tipos según el número de unos que contengan, de manera que pudiésemos hacer lo siguiente: primero, contar la fila que no tiene ningún uno, a continuación, todas las filas con exactamente un 1, a renglón seguido, todas las filas con exactamente dos unos y así sucesivamente hasta contar una última fila con todos uno. El número total de filas cada una de las cuales contiene exactamente k unos es $PR_{k,10-k}$ (contiene k unos repetidos y $10-k$ ceros repetidos). El número que nos interesa es

$$n = \sum_{k=0}^{10} PR_{k,10-k},$$

o lo que es lo mismo,

$$n = \sum_{k=0}^{10} \binom{10}{k} \tag{19.1}$$

—la explicación de $\binom{10}{k}$ como problema de distribución/ocupación es que se trata de distribuir k objetos no distinguibles (los k unos) en 10 recipientes distinguibles (las 10 posiciones de cualquier fila de la matriz) sin importar el orden de colocación de los objetos dentro de los recipientes, ocurriendo que en ingún recipiente hay más de un objeto, esto es, la aplicación subyacente es inyectiva (no obstante, observemos que al ser indistinguibles los objetos, aunque distintos, el «conjunto» de objetos, dominio de la aplicación, es en realidad un multiconjunto)—. Es un resultado conocido que, para cualquier $n \in \mathbb{N}$:

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n,$$

por tanto, (19.1) es igual a 2^{10}. ■

Ejemplo 696

Sean X e Y dos conjuntos finitos no vacíos de cardinales respectivos x e y. ¿Cuántas correspondencias existen de X a Y? Respondamos a esta cuestión incluyendo en nuestro razonamiento el principio de la adición.

[EFO 24.5.2023:7].

Resolución.—

1. *Discusión previa.*

   Una correspondencia de X a Y es una relación de X a Y, en definitiva, un subconjunto del producto cartesiano $X \times Y$, por lo que el número de correspondencias de X a Y es igual al número de subconjuntos de $X \times Y$.

Por otra parte, un subconjunto de $X \times Y$ es una combinación de elementos de $X \times Y$, concretamente, un subconjunto de k elementos de $X \times Y$ es una combinación de k elementos de $X \times Y$.

Tenemos, pues, que el número de correspondencias es el número de combinaciones de k elementos de $X \times Y$, para todos los k tales que $0 \leq k \leq xy$, pues el cardinal de $X \times Y$ es xy.

Calculemos este número mediando el principio de la adición.

II. *Formalización del principio de la adición.*

Para poder aplicar el principio de la adición debemos definir sucesos incompatibles dos a dos. Estos sucesos son:

$$\begin{aligned} S_0 &\leftrightharpoons \text{ser un subconjunto de } X \times Y \text{ de cardinal } 0; \\ S_1 &\leftrightharpoons \text{ser un subconjunto de } X \times Y \text{ de cardinal } 1; \\ &\vdots \\ S_{xy} &\leftrightharpoons \text{ser un subconjunto de } X \times Y \text{ de cardinal } xy; \end{aligned}$$

que son incompatibles dos a dos, puesto que un subconjunto no puede tener cardinales distintos.

III. *De las formas de suceder los sucesos.*

Como el número de subconjuntos de k elementos de $X \times Y$ es el número de combinaciones de k elementos de $X \times Y$, el suceso S_k sucede de $C(xy, k)$ formas distintas.

IV. *Aplicación del principio de la adición.*

Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_0 \cup S_1 \cup \ldots \cup S_{xy}$. Como hemos dicho ya, son sucesos incompatibles dos a dos —ya que un subconjunto no puede tener cardinales distintos—, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

$$\begin{aligned} \#(S_0 \cup S_1 \cup \ldots \cup S_{xy}) &= \#S_0 + \#S_1 + \ldots + \#S_{xy} \\ &= \binom{xy}{0} + \binom{xy}{1} + \ldots + \binom{xy}{xy}. \end{aligned}$$

Solución.— Existen $\displaystyle\sum_{k=0}^{xy} \binom{xy}{k}$ correspondencias de un conjunto finito de cardinal x a un conjunto finito de cardinal y. ■

Observación 19.6.0.— La suma $\binom{xy}{0} + \binom{xy}{1} + \ldots + \binom{xy}{xy}$ es igual a 2^{xy} (propiedad del cardinal del conjunto potencia).

Ejemplo 697

¿Cuántas palabras de siete letras pueden formarse con las 27 letras del alfabeto español si cada palabra contiene dos, tres o cinco vocales?

[EFE 7.7.2017:6a], [SEL 11:2]. *Cfr.* Brualdi [217]: ejemplo (pág. 43).

Resolución.—

I. *Discusión previa*.

No la haremos; simplemente diremos que lo resolveremos por el principio de la adición, calculando el número pedido en los tres casos considerados.

II. *Formalización del principio de la adición*.

Para poder aplicar el principio de la adición debemos definir sucesos incompatibles dos a dos. Estos sucesos son:

$$S_2 \coloneqq \text{ser una palabra española de 7 letras que contiene exactamente 2 vocales;}$$
$$S_3 \coloneqq \text{ser una palabra española de 7 letras que contiene exactamente 3 vocales;}$$
$$S_5 \coloneqq \text{ser una palabra española de 7 letras que contiene exactamente 5 vocales;}$$

que son incompatibles dos a dos, puesto que una palabra sólo tiene un número determinado de vocales.

III. *De las formas de suceder los sucesos*.

A. Pensemos en dos vocales.

Formalmente, para aplicar el principio de la multiplicación, tenemos que definir un suceso descompuesto en fases sucesivas e independientes.

Lo tenemos. El suceso

$$S_2 \coloneqq \text{ser una palabra española de 7 letras que contiene exactamente 2 vocales,}$$

que ocurre en tres fases sucesivas e independientes:

- fase S_{20}, «la elección de las posiciones de las dos vocales», que existen $\binom{7}{2}$ formas distintas de llevarla a cabo;
- fase S_{21}: «el "relleno" de las dos posiciones de las vocales, que existen 5^2 formas distintas de efectuarlo;
- fase S_{22}: «el "relleno" de las posiciones de las consonantes», que existen 22^{7-2} formas distintas de realizarlo.

Así, aplicando el principio de la multiplicación, existen

$$\binom{7}{2}5^2 22^{7-2} = 2\,705\,656\,800. \tag{19.2}$$

formas de que ocurra el suceso S_2, esto es, justamente ese es el número de palabras españolas de siete letras con dos vocales.

B. Un razonamiento similar nos lleva a que el número de formas de que suceda el suceso S_3, esto es, el número de palabras españolas de siete letras con tres vocales es

$$\binom{7}{3}5^3 22^{7-3} = 1\,024\,870\,000, \tag{19.3}$$

C. y similarmente el número de formas de que suceda el suceso S_5, esto es, el número de palabras españolas de siete letras con cinco vocales es

$$\binom{7}{5}5^5 22^{7-5} = 31\,762\,500. \tag{19.4}$$

IV. *Aplicación del principio de la adición.*

De (19.2), (19.3) y (19.4), por el principio de la adición (los sucesos S_2, S_3 y S_5, esto es, tener exactamente dos vocales, tres o cinco, son sucesos incompatibles dos a dos) se sigue que el número de palabras buscado es la suma de los números de formas en que suceden dichos sucesos, es decir,

$$2\,705\,656\,800 + 1\,024\,870\,000 + 31\,762\,500 = 3\,762\,289\,300.$$

Solución.— Existen 3 762 289 300 palabras españolas de siete letras que contienen dos, tres o cinco vocales. ■

Ejemplo 698

Una urna contiene siete bolas numeradas del uno al siete. Las bolas se extraen todas, de una en una y sin reposición. A la par de las extracciones, se escriben las cifras resultantes por orden de salida y de izquierda a derecha. Razonemos con argumentos combinatorios cuántos números así formados empiezan y terminan por cifra par.

Resolución.—

I. *Discusión previa.*

Hay siete posiciones. En los extremos, las hipótesis obligan cifra par. Hay tres cifras pares entre 1 y 7, a saber, 2, 4 y 6. Guiándonos, por ejemplo, por la modelización II, pensemos en estos tres números (cajas distinguibles) y en los dos extremos (objetos distinguibles), con la condición de

ser inyectiva la aplicación subyacente (como mucho un extremo por número, ya que no hay bolas con el mismo número).

Para cada uno de estos casos en los extremos (cada una de las variaciones) tenemos que considerar todas las posibilidades en las cinco posiciones intermedias. Estas posibilidades son las permutaciones de cinco elementos (una nueva abstracción como cinco objetos distinguibles [las posiciones intermedias] en cinco recipientes distinguibles [los números 1, 3 y 5 y el número par no presente en los extremos], esta vez siendo biyectiva la aplicación).

Para formalizar lo anterior, aplicamos el *principio de la multiplicación*.

II. *Formalización del principio de la multiplicación*.

Sea el suceso

$S \coloneqq$ formar un número de siete cifras con las cifras de 1 a 7 siendo par la cifra inicial y la final,

cuya ocurrencia definimos en dos fases sucesivas e independientes (cada fase de cómo se haya realizado la fase anterior, no necesariamente de qué se haya realizado). El suceso S se lleva a término en estas dos fases:

$S_0 \coloneqq$ situar dos de los números pares 2, 4 y 6 en los extremos;

$S_1 \coloneqq$ situar en las cinco posiciones intermedias los números 1, 3 y 5 y el número par no situado en los extremos.

III. *De las formas de realizar cada fase*.

La fase S_0 se hace de $V(3, 2)$ formas. La fase S_1, de $P(5)$ formas.

IV. *Aplicación del principio de la multiplicación*.

Notando por $\#X$, tanto el número de formas en que puede suceder el suceso X como el número de formas en que puede realizarse la fase X,

$$\begin{aligned}\#S &= \#S_0 \cdot \#S_1 \\ &= V(3,2) \cdot P(5) \\ &= 3^{\underline{2}} \cdot 5! \\ &= (3 \cdot 2) \cdot (5!) \\ &= 6 \cdot 120 \\ &= 720.\end{aligned}$$

Solución.— 720 números. ■

Ejemplo 699

En una reunión de diecisiete personas se realiza una votación secreta. Siete de ellas han emitido un voto favorable, cinco han votado en contra, tres un voto en blanco y dos un voto nulo. Razonemos con argumentos combinatorios de cuántas formas ha podido suceder esto.

[Cubit 145].

Resolución.—

I. *Discusión previa.*

Usemos la modelización II, representando las bolas y las cajas a los votos y las personas, respectivamente. Pensemos en las 17 personas (cajas distinguibles) y los siete votos síes (bolas indistinguibles), con la condición de ser inyectiva la aplicación subyacente (no más de un voto por persona) —alternativamente, es posible pensar en el número de subconjuntos de siete elementos de un conjunto de 17 elementos—. De cualquier forma, resultan $C(17, 7)$ maneras de distribuir los votos síes en las cajas.

Para cada uno de los casos (cada una de las combinaciones), quedan diez cajas vacías. Ahora, razonando similarmente, hay $C(10, 5)$ formas de distribuir los votos noes en las cajas, quedando, para cada uno de los casos, cinco cajas vacías.

Análogamente, hay $C(5, 3)$ maneras de distribuir los votos en blanco en las cajas, quedando, para cada uno de los casos, dos cajas vacías.

Igualmente, hay $C(2, 2)$ formas de colocar los votos nulos en las cajas.

Para formalizar lo anterior, aplicamos el *principio de la multiplicación*.

II. *Formalización del principio de la multiplicación.*

Sea el suceso

$S \leftrightharpoons$ formar un resultado de una votación de 17 personas con siete votos a favor, cinco en contra, tres en blanco y dos nulos,

cuya ocurrencia definimos en cuatro fases sucesivas e independientes (cada fase de cómo se haya realizado la fase anterior, no necesariamente de qué se haya realizado). El suceso S se lleva a término en estas cuatro fases:

$$S_0 \leftrightharpoons \text{siete de diecisiete personas votan sí;}$$
$$S_1 \leftrightharpoons \text{cinco de diez personas votan no;}$$
$$S_2 \leftrightharpoons \text{tres de cinco personas votan en blanco;}$$

$$S_3 \leftrightharpoons \text{el voto de dos de dos personas es nulo.}$$

III. *De las formas de realizar cada fase.*

La fase S_0 se hace de $C(17,7)$ formas; S_1, de $C(10,5)$ formas; S_2, de $C(5,3)$ formas y S_3 de $C(2,2)$ formas.

IV. *Aplicación del principio de la multiplicación.*

Notando por $\#X$, tanto el número de formas en que puede suceder el suceso X como el número de formas en que puede realizarse la fase X,

$$\begin{aligned}
\#S &= \#S_0 \cdot \#S_1 \cdot \#S_2 \cdot \#S_3 \\
&= C(17,7) \cdot C(10,5) \cdot C(5,3) \cdot C(2,2) \\
&= \binom{17}{7} \cdot \binom{10}{5} \cdot \binom{5}{3} \cdot \binom{2}{2} \\
&= \frac{17!}{7! \cdot 10!} \cdot \frac{10!}{5! \cdot 5!} \cdot \frac{5!}{3! \cdot 2!} \cdot \frac{2!}{2! \cdot 0!} \\
&= \frac{17! \cdot \cancel{10!} \cdot \cancel{5!} \cdot \cancel{2!}}{7! \cdot \cancel{10!} \cdot \cancel{5!} \cdot 5! \cdot 3! \cdot \cancel{2!} \cdot 2! \cdot 0!} \\
&= 49\,008\,960.
\end{aligned}$$

Solución.— De 49 008 960 formas. ■

Ejemplo 700

Nos preguntamos:

0. ¿De cuántas formas puede un computador central c_0 repartir doce tareas indistinguibles entre cinco computadores auxiliares $c_1, \ldots, c_5$?
1. ¿Y si no le está permitido a c_0 asignar más de siete tareas a ningún computador auxiliar?

0: [EFO 1.6.2017:5a], [EFE 28.6.2023:7].

Resolución.—

0. Sea $C = \{c_1, c_2, \ldots, c_5\}$ el conjunto de los cinco computadores auxiliares. Un reparto no es más que un multiconjunto de elementos de C de cardinalidad doce; por ejemplo, el reparto de dos tareas a c_2, tres tareas a c_3 y siete tareas a c_5 es el multiconjunto $\{\{c_2, c_2, c_3, c_3, c_3, c_5, c_5, c_5, c_5, c_5, c_5, c_5\}\}$; así, por definición de combinación con repetición, un reparto es una combinación con repetición de orden doce de elementos de C, por lo que el número de repartos es el número de combinaciones con repetición de orden doce de elementos

de C y este número, por un teorema conocido, es

$$\begin{aligned} CR(5,12) &= \binom{5+12-1}{12} \\ &= \frac{16!}{12!\cdot 4!} \\ &= \frac{16\cdot 15\cdot 14\cdot 13\cdot \cancel{12!}}{\cancel{12!}\cdot 4!} \\ &= \frac{4\cdot \cancel{4}\cdot 5\cdot \cancel{3}\cdot 7\cdot \cancel{2}\cdot 13}{\cancel{4}\cdot \cancel{3}\cdot \cancel{2}} \\ &= 4\cdot 5\cdot 7\cdot 13 \\ &= 1820. \end{aligned}$$

Solución.— Un computador central puede repartir doce tareas indistinguibles entre cinco computadores auxiliares de 1820 formas.

1. Ejemplo de una asignación de tareas permitida es siete tareas a c_1, cinco a c_2 y ninguna a cada uno de los demás, y de una no permitida es ocho tareas a c_1 y una a cada uno de los demás.

   Aplicaremos el principio del complementario.

   I. *Formalización del principio del complementario*.

      Para poder aplicar el principio del complementario necesitamos un conjunto y un subconjunto suyo. Sea el conjunto B de los repartos sin ninguna restricción y su subconjunto A de los repartos en los que ningún computador auxiliar recibe más de siete tareas. Entonces el complementario de A en B, $B \setminus A$, es el conjunto de repartos en los que algún computador auxiliar recibe más de siete tareas.

   II. *De los cardinales* $|B|$ *y* $|B \setminus A|$.

      Del apartado anterior sabemos que $|B| = 1820$. Calculemos ahora $|B \setminus A|$. Apliquemos el principio de la multiplicación.

      A. *Formalización del principio de la multiplicación*.

         Para poder aplicar el principio de la multiplicación debemos definir la ocurrencia del suceso S de repartir en varias fases sucesivas e independientes (cada fase de cómo se haya realizado la fase anterior, no necesariamente de qué se haya realizado). El suceso de repartir se lleva a término en estas dos fases:

         $S_0 \leftrightharpoons$ repartir 8 tareas a un computador auxiliar;

         $S_6 \leftrightharpoons$ repartir las 4 tareas sobrantes entre los 5 computadores auxiliares.

      B. *De las formas de realizar cada fase*.

La fase S_0 se hace de cinco formas, por haber cinco computadores auxiliares. Apliquemos el principio de la adición.

0. *Formalización del principio de la adición.*

   Para poder aplicar el principio de la adición debemos definir sucesos incompatibles dos a dos,

$$S_i \coloneqq \text{repartir 8 tareas al computador auxiliar } c_i,$$

   para $i \in \{1, 2, 3, 4, 5\}$, cinco sucesos incompatibles dos a dos, puesto que se trata de computadores distintos.

1. *De las formas de suceder los sucesos.*

   De ser indistinguibles las tareas se sigue que sólo exista una forma de repartir 8 tareas a un computador auxiliar, en otras palabras, los sucesos S_i sólo suceden una vez, esto es, $\forall i \in \{1, 2, 3, 4, 5\}, \#S_i = 1$.

2. *Aplicación del principio de la adición.*

   Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5$. Como hemos dicho ya, son sucesos incompatibles dos a dos, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

$$\begin{aligned}\#(S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5) &= \#S_1 + \#S_2 + \#S_3 + \#S_4 + \#S_5 \\ &= 1 + 1 + 1 + 1 + 1 \\ &= 5.\end{aligned}$$

La fase S_6 se realiza de $CR(5, 4)$ formas, siendo el razonamiento análogo al del apartado 0, esta vez repartiendo cuatro tareas en vez de doce.

C. *Aplicación del principio de la multiplicación.*

Notando por $\#X$, tanto el número de formas en que puede suceder el suceso X como el número de formas en que puede realizarse la fase X,

$$\begin{aligned}\#S &= \#S_0 \cdot \#S_6 \\ &= 5 \cdot CR(5, 4) \\ &= 5 \cdot \binom{5 + 4 - 1}{4} \\ &= 5 \cdot \frac{8!}{4! \cdot 4!}\end{aligned}$$

$$= 5 \cdot \frac{\cancel{4} \cdot 2 \cdot 7 \cdot \cancel{3} \cdot \cancel{2} \cdot 5 \cdot \cancel{4!}}{\cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot \cancel{4!}}$$
$$= 5 \cdot 2 \cdot 7 \cdot 5$$
$$= 350.$$

III. *Aplicación del principio del complementario.*

$$|A| = |B| - |B \setminus A|$$
$$= 1820 - 350$$
$$= 1470.$$

Solución.— Un computador central puede repartir doce tareas indistinguibles entre cinco computadores auxiliares, con la condición de que ninguno de estos últimos reciba más de siete tareas, de 1470 formas. ■

Observación 19.6.1.— Como es lógico, la imposición de una restricción hace que el número de formas sea menor: 1470 frente a 1820.

Observación 19.6.2.— Pudiésemos formular lo buscado en el apartado I como el número de soluciones no negativas de la ecuación $x_1 + x_2 + x_3 + x_4 + x_5 = 12$ siendo $\forall i \in \{1, 2, 3, 4, 5\}$, $x_i \leq 7$. Sin embargo, su resolución es más complicada[31].

Ejemplo 701

En una prueba de rendimiento, un computador central c_0 debe distribuir 100 tareas idénticas a un centro de datos de 30 computadores de tipo A y 20 computadores de tipo B, requiriéndose que cada computador de tipo A tenga al menos una tarea asignada y que cada computador de tipo B tenga al menos dos tareas asignadas. ¿De cuántas formas puede hacer c_0 tal distribución?

[EFE 7.7.2017:6b], [SEL 11:3]. *Cfr.* CAMERON [218]: ejemplo (pág. 18).

Resolución.— Una forma de calcularlo es que c_0 primero reparta una tarea a cada computador de tipo A y dos tareas a cada computador de tipo B; en total, $30 + 2 \cdot 20 = 70$ tareas. Ahora, quedan por distribuir las 30 restantes entre los 50 computadores, lo cual puede hacerse de

$$CR(50, 30) = \binom{50 + 30 - 1}{30}$$

[31] *Vid. v. gr.* http://math.stackexchange.com/questions/992125/rolling-dice-problem/1680420#1680420.

$$= \binom{79}{30}$$
$$= 5\,544\,632\,834\,275\,283\,414\,380$$

formas. ■

Ejemplo 702

¿De cuántas formas pueden colocarse alineadas las cinco cifras decimales pares y las cinco cifras decimales impares de manera que no haya dos cifras decimales impares juntas?

[EFO 3.6.2019:5a], [EFEC 29.1.2025:12] (tipo test).

Resolución.— Lo resolvemos aplicando el principio de la multiplicación. Sea el suceso $S \leftrightharpoons$ colocar alineadas las cinco cifras decimales pares y las cinco cifras decimales impares de manera que no haya dos cifras decimales impares juntas. Es posible descomponer la ocurrencia de S en dos fases consecutivamente independientes S_0 y S_1: inicialmente, colocamos libremente los pares, lo cual puede hacerse de $\#S_0$ formas y, a continuación, colocamos los impares sujetos a la condición dada, lo cual puede hacerse de $\#S_1$ formas; entonces, por el principio de la multiplicación, la colocación completa (el suceso S) se realiza de $\#S_0 \cdot \#S_1$ formas.

Pensemos cada fase en el ámbito, por ejemplo, de la modelización II.

Colocación de los pares.— El número total de disposiciones en línea de las cifras pares es $5!$. En efecto, esto es así porque como problema de distribución/ocupación se trata de distribuir 5 objetos distinguibles (las cifras) en 5 recipientes distinguibles (sus posiciones) sin importar el orden de colocación de los objetos dentro de los recipientes (ya que sólo hay una cifra por posición), ocurriendo que la colocación está sujeta a esto último, esto es, la aplicación subyacente debe ser inyectiva, pero también sobreyectiva —y, por tanto, biyectiva— al ser iguales el número de cifras que el de posiciones. En definitiva, $\#S_0 = 5$.

Colocación de los impares.— Para cada disposición en línea de las cifras pares, quedan 6 posiciones distintas para las cifras impares (1 posición delante + 4 posiciones en medio + 1 posición detrás). Tenemos así que, como problema de distribución/ocupación, se trata de distribuir 5 objetos distinguibles (las 5 cifras impares) en 6 recipientes distinguibles (las 6 posiciones distintas) sin importar el orden de colocación de los objetos dentro de los recipientes (ya que al no poder aparecer juntas, sólo hay una cifra impar por posición), ocurriendo que la colocación está sujeta a esto último, esto es, la aplicación subyacente debe ser inyectiva (y necesariamente no sobreyectiva al haber más posiciones que cifras impares). Según un teorema conocido (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198

de esta edición)—), en este caso, el número total de distribuciones es

$$\begin{aligned} V(6,5) &= 6^{\underline{5}} \\ &= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \\ &= 720. \end{aligned}$$

Aplicando finalmente el principio de la multiplicación, obtenemos que el número buscado es

$$5! \cdot 720 = 86\,400.$$

Solución.— De 86 400 formas. ■

Ejemplo 703

Sea que disponemos de diez ejemplares del *Quijote*, todos de la misma tirada. Imaginemos también un mueble librería de cuatro estantes, digamos a, b, c y d y supongamos que todos los libros caben en cualquiera de éstos y que, consecuentemente, podrían quedar estantes vacíos. ¿De cuántas formas pudiésemos colocar estos diez ejemplares en los estantes de esta librería, suponiendo que:

0. tal colocación no está sujeta a restricciones?
1. en todos los estantes tiene que haber al menos un ejemplar?
2. en el estante b debe haber al menos tres ejemplares y en el estante d exactamente dos?

[EPF 14.5.2019:5].

Resolución.— Razonemos en el ámbito, por ejemplo, de la modelización II.

0. Como problema de distribución/ocupación, se trata de distribuir 10 objetos no distinguibles (los 10 ejemplares) en 4 recipientes distinguibles (los 4 estantes) sin importar el orden de colocación de los objetos (libros) dentro de los recipientes (en los estantes), ocurriendo que la colocación no está sujeta a restricciones, esto es, la aplicación subyacente es cualquiera —observemos que si bien los objetos son indistinguibles, son distintos (como las bolas del mismo color en una piscina de bolas de colores), por lo que la colección de objetos puede considerarse un conjunto [que no multiconjunto] y como tal, conjunto original y dominio de la aplicación subyacente—. En definitiva, el número de formas es

$$\begin{aligned} CR_{4,10} &= \binom{4+10-1}{10} \\ &= \frac{13!}{10! \cdot 3!} \end{aligned}$$

$$
\begin{aligned}
&= \frac{13 \cdot 12 \cdot 11 \cdot \cancel{10!}}{\cancel{10!} \cdot 3 \cdot 2} \\
&= 286.
\end{aligned}
$$

1. La única diferencia con el apartado anterior, es que, al exigirse que se coloque al menos un ejemplar en cada estante, la aplicación subyacente es sobreyectiva. De acuerdo con los teoremas conocidos en el ámbito de la modelización como problema de distribución/ocupación, se tiene que dicho número de formas es

$$
\begin{aligned}
CR_{4,10-4} &= \binom{10-1}{4-1} \\
&= \frac{9!}{3! \cdot 6!} \\
&= \frac{9 \cdot 8 \cdot 7 \cdot \cancel{6!}}{3 \cdot 2 \cdot \cancel{6!}} \\
&= 84.
\end{aligned}
$$

Observemos también el razonamiento de haber satisfecho la restricción al comienzo, situando un libro en cada estante, por lo que quedarían $10-4$ libros a repartir entre todos los estantes, ahora sin restricciones. Así, hemos reducido[32]el problema descrito en el apartado 1 al descrito en el apartado 0 y la solución es la de éste para el caso de $10-4$ libros y 4 estantes.

2. La situación descrita equivale a colocar 5 ejemplares (10 menos los 3 que están en b menos los 2 que están en d) en los 3 estantes a, b y c (en d no puede colocarse ninguno más). Esto es, de nuevo todo consiste en satisfacer las restricciones al comienzo. Como problema de distribución/ocupación, se trata de distribuir 5 objetos no distinguibles (los 5 ejemplares) en 3 recipientes distinguibles (los 3 estantes) sin importar el orden de colocación de los objetos (libros) dentro de los recipientes (en los estantes), y como las exigencias fueron satisfechas al principio, ocurre que la colocación no está sujeta a restricciones, esto es, la aplicación subyacente es cualquiera —de nuevo, observemos que si bien los objetos son indistinguibles, son distintos (como las bolas del mismo color en una piscina de bolas de colores), por lo que la colección de objetos puede considerarse un conjunto [que no multiconjunto] y como tal, conjunto original y dominio de la aplicación subyacente—. En definitiva, el número de formas es

$$
\begin{aligned}
CR_{3,5} &= \binom{3+5-1}{5} \\
&= \frac{7!}{5! \cdot 2!} \\
&= \frac{7 \cdot 6 \cdot \cancel{5!}}{\cancel{5!} \cdot 2} \\
&= 21.
\end{aligned}
$$



[32] *Vid. v. gr.* https://es.wikipedia.org/wiki/Reducci%C3%B3n_(complejidad).

Ejemplo 704

¿De cuántas formas pueden escogerse 7 cifras decimales distintas,

I. de las que 4 sean pares y 3 impares?
II. de las que a lo sumo 4 sean pares?
III. si debe haber al menos 3 cifras pares y exactamente 2 impares?

[EFO 3.6.2019:5b].

Resolución.— Razonemos en el ámbito, por ejemplo, de la modelización II.

Vistos como problemas de distribución/ocupación estos problemas de selección —dos en el apartado I, seis en el II y dos en el III—, se trata de distribuir objetos indistinguibles —el número de cifras deseado: I, 4 y 3; II, 2, 5, 3, 4, 4 y 3; III, 5 y 2— en recipientes distinguibles (siempre 5, el número total de cifras, pares o impares, sin mezclar) (observemos que escoger k cifras de las 5 es como situar una bola, indistinguible, en k de los 5 recipientes).

Además, no importa el orden de colocación de los objetos dentro de los recipientes (ya que cada cifra sólo cuenta una vez) y ocurre que la colocación está sujeta a esto último, esto es, la aplicación subyacente debe ser inyectiva (y necesariamente no sobreyectiva al ser siempre el número de cifras deseado menor que el total de cifras).

Siendo k el número de objetos y n el de recipientes, según un teorema conocido (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—), el número total de distribuciones es el número total de combinaciones de n elementos tomados de k en k. Así pues, tenemos que:

I. de las 5 cifras pares elegibles, es posible escoger las 4 de un total de $C(5,4)$ formas, y por cada una de éstas hay $C(5,3)$ formas de escoger las cifras impares; por lo tanto, al tratarse de dos fases consecutivamente independientes, aplicamos el principio de la multiplicación y el número buscado es

$$\underbrace{\binom{5}{4}}_{pares}\cdot\underbrace{\binom{5}{3}}_{impares} = \frac{5!}{1!\cdot 4!}\cdot\frac{5!}{2!\cdot 3!}$$
$$= \frac{5\cdot \cancel{4!}}{1\cdot \cancel{4!}}\cdot\frac{5\cdot 4\cdot \cancel{3!}}{2\cdot \cancel{3!}}$$
$$= 5\cdot 10 = 50;$$

II. la restricción de que a lo sumo 4 sean pares y el total de 7 cifras se traduce en las posibilidades: 2 pares y 5 impares, 3 pares y 4 impares o 4 pares y 3 impares, siendo las tres situaciones mutuamente excluyentes y dividiéndose cada situación en dos fases consecutivamente independientes; aplicando el principio de la adición a las tres situaciones y el de la multiplicación a cada una,

el número buscado es

$$\begin{aligned}&\underbrace{\binom{5}{2}}_{\text{pares}}\cdot\underbrace{\binom{5}{5}}_{\text{impares}}+\underbrace{\binom{5}{3}}_{\text{pares}}\cdot\underbrace{\binom{5}{4}}_{\text{impares}}+\underbrace{\binom{5}{4}}_{\text{pares}}\cdot\underbrace{\binom{5}{3}}_{\text{impares}}\\&=10\cdot 1+10\cdot 5+5\cdot 10\\&=110;\end{aligned}$$

III. si debemos escoger 7 cifras decimales y debe haber exactamente 2 impares y al menos 3 pares, entonces sólo cabe la posibilidad de que el número de cifras pares sea 5; éstas son dos fases consecutivamente independientes del suceso pedido; aplicando el principio de la multiplicación, tenemos que el número buscado es

$$\underbrace{\binom{5}{5}}_{\text{pares}}\cdot\underbrace{\binom{5}{2}}_{\text{impares}}=1\cdot 10=10,$$

número que corresponde a los 10 subconjuntos de elección siguientes:

$$\begin{aligned}&\{0,2,4,6,8\}\cup\{1,3\},\\&\{0,2,4,6,8\}\cup\{1,5\},\\&\{0,2,4,6,8\}\cup\{1,7\},\\&\{0,2,4,6,8\}\cup\{1,9\},\\&\{0,2,4,6,8\}\cup\{3,5\},\\&\{0,2,4,6,8\}\cup\{3,7\},\\&\{0,2,4,6,8\}\cup\{3,9\},\\&\{0,2,4,6,8\}\cup\{5,7\},\\&\{0,2,4,6,8\}\cup\{5,9\},\\&\{0,2,4,6,8\}\cup\{7,9\}.\end{aligned}$$



Ejemplo 705

Supongamos una red en forma de polígono de n nodos (vértices). Calculemos n, sabiendo que el número de aristas (lados + diagonales) es 253.

[EFE 7.7.2017:5b].

Resolución.— Siendo n el número de nodos, el número de aristas es el número de subconjuntos de dos elementos —cada arista al unir dos nodos, puede abstraerse como un subconjunto de dos elementos— de un conjunto de n elementos (los n nodos), esto es, por definición de combinación,

dicho número es $C(n,2)$. Entonces: $C(n,2) = 253 \to n(n-1)/2 = 253 \to n = -22 \vee n = 23$, de donde, al no poder ser negativo el número de nodos, $n = 23$. ■

Ejemplo 706

Sean siete rectas coplanarias tales que tres cualesquiera de ellas no pertenecen al mismo haz de rectas. Si tres de ellas son paralelas, ¿cuántos puntos de corte determinan en total?

Resolución.— Lo resolvemos por el principio de la adición [¡esto requiere justificación! ✍]. Obviemos temporalmente dos de las tres rectas paralelas. Las otras cinco se cortan en $C(5,2) = 10$ puntos —el número de puntos de corte es el número total de subconjuntos de dos elementos (cada punto de corte lo es de dos rectas) de un conjunto de cinco elementos (las cinco rectas)—; como cada una de las dos rectas restantes corta a las demás en cuatro puntos, en total existen $10 + 4 + 4 = 18$ puntos de corte. ■

Actividad 19.22

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Ejemplo 707

Queremos repartir 25 sillas en cuatro habitaciones vacías. ¿De cuántas formas podemos hacerlo en los siguientes casos?

0. No podemos dejar ninguna habitación sin sillas,
   a. siendo capaces de distinguir las sillas entre sí,
   b. no siendo capaces de distinguir las sillas entre sí;
1. podemos dejar habitaciones sin sillas,
   a. siendo capaces de distinguir las sillas entre sí,
   b. no siendo capaces de distinguir las sillas entre sí.

[EFE 29.6.2018:5].

Resolución.— Razonemos en el ámbito, por ejemplo, de la modelización II.

0. La aplicación del conjunto o multiconjunto de objetos (el conjunto de sillas) en el conjunto de recipientes ()el conjunto de habitaciones) es sobreyectiva, pues en todo recipiente hay al menos un objeto (no puede dejarse ninguna habitación sin sillas).

a. Son 25 objetos distinguibles (las sillas pueden distinguirse entre sí) a distribuir en cuatro recipientes distinguibles (las habitaciones); como parece entenderse que los repartos se diferencian únicamente por el número de sillas por habitación, entonces el orden de los objetos dentro de cada recipiente no importa (distribución no ordenada). Entonces (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—)

$$\begin{aligned} 4!S(25,4) &= 4!\left(\frac{1}{4!}\sum_{i=0}^{4-1}(-1)^i\binom{4}{i}(4-i)^{25}\right) \\ &= 4!\cdot 46771289738810 \\ &= 1122510953731440. \end{aligned}$$

b. Son 25 objetos indistinguibles (las sillas no pueden distinguirse entre sí) a distribuir en cuatro recipientes distinguibles (las habitaciones); por ser los objetos indistinguibles, su orden dentro de cada recipiente no importa (distribución no ordenada). Entonces (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—)

$$\begin{aligned} CR(4,25-4) &= \binom{(25-4)+4-1}{4-1} \\ &= \frac{24\cdot 23\cdot 22\cdot 21!}{3\cdot 2\cdot 21!} \\ &= 2024. \end{aligned}$$

Recordemos que $CR(n,k) = C(k+n-1, n-1)$.

1. La aplicación del conjunto o multiconjunto de objetos (el conjunto de sillas) en el conjunto de recipientes (el conjunto de habitaciones) no tiene ninguna restricción, pues sólo se dice que pueden dejarse recipientes vacíos (pueden dejarse habitaciones sin sillas), esto es, puede ser o no ser sobreyectiva y, por otro lado, nada se dice sobre la inyectividad, esto es, sobre si, caso de haber, puede o no haber más de un objeto en un recipiente. Se trata, pues, de una aplicación cualquiera.

a. Son 25 objetos distinguibles (las sillas pueden distinguirse entre sí) a distribuir en cuatro recipientes distinguibles (las habitaciones); como parece entenderse que los repartos se diferencian únicamente por el número de sillas por habitación, el orden de los objetos dentro de cada recipiente no importa (distribución no ordenada). Entonces (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—)

$$\begin{aligned} VR(4,25) &= 4^{25} \\ &= 1125899906842624. \end{aligned}$$

b. Son 25 objetos indistinguibles (las sillas no pueden distinguirse entre sí) a distribuir en cuatro recipientes distinguibles (las habitaciones); por ser los objetos indistinguibles, su

orden dentro de cada recipiente no importa (distribución no ordenada). Entonces (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—)

$$\begin{aligned} CR(4,25) &= \binom{4+25-1}{25} \\ &= \frac{28 \cdot 27 \cdot 26 \cdot 25!}{3 \cdot 2 \cdot 25!} \\ &= 3276. \end{aligned}$$

Recordemos que $CR(n,k) = C(n+k-1,k)$. ■

. . . .

En los siguientes cinco ejemplos, debemos hallar justificadamente el número de iteraciones del bucle interno mediante al menos un razonamiento combinatorio.

El lenguaje es PSeInt[33].

. . . .

[33] *Cfr. supra* § 11 (pág. cii de esta edición).

Ejemplo 708

```
// subproceso que devuelve el número de iteraciones del bucle interno
SubProceso res <- f()
    res <- 0 // inicialización del contador de iteraciones
    // dos iteraciones anidadas
    i <- 1
    Mientras i < 1234 Hacer
        j <- 0
        Mientras j < 123 Hacer
            res <- res + 1 // incremento del contador de iteraciones
            j <- j + 1
        FinMientras
        i <- i * 2
        i <- i + 1
    FinMientras
FinSubProceso

Proceso numdeiterbucleinterno
    Escribir "El n.º de iteraciones del bucle interno es ", f()
FinProceso
```

[CEOV 2020-2021, 2021-2022 (p.h.e.c.)].

Resolución.— Los bucles no son interdependientes, por lo que es admisible aplicar el principio de multiplicación, interpretando dichos bucles como fases: el programa es el suceso y la ejecución de aquél es la ocurrencia de éste, ocurrencia que tiene lugar en dos fases cuyas realizaciones se plasman en las ejecuciones del bucle externo e interno, respectivamente.

El bucle externo (i) recorre 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024. Como debe ser menor que 1234, se detiene cuando llega a 2048. Eso es un total de 11 iteraciones (puede obtenerse calculando $\log_2 2048$).

Para cada una de las iteraciones anteriores, el bucle interno (j) recorre $0, 1, 2, 3, \dots, 123$, esto es, un total de 124 iteraciones.

Por el principio de la multiplicación, el número de iteraciones del bucle interno es $11 \cdot 124 = 1364$. ■

Ejemplo 709

```
// subproceso que recibe el argumento n por valor
// y devuelve el número de iteraciones del bucle interno
SubProceso res <- f(n Por Valor)
    res <- 0 // inicialización del contador de iteraciones
    // dos iteraciones anidadas
    Para i Desde 0 Hasta n - 1 Con Paso 1 Hacer
        Para j Desde i + 1 Hasta n - 1 Con Paso 1 Hacer
            res <- res + 1 // incremento del contador de iteraciones
        FinPara
    FinPara
FinSubProceso

Proceso numdeiterbucleinterno
    Escribir "Introduzca un n.º entero positivo"
    Leer n
    Escribir "El n.º de iteraciones del bucle interno es ", f(n)
FinProceso
```

[CEOV 2020-2021, 2021-2022 (p.h.e.c.)].

Resolución.— Pensemos en lo que sucede en cada iteración del bucle externo. Inicialmente, cuando el valor de i es 0, el bucle interno (j) comienza en 1 y se procesa hasta $n-1$, esto es, se desarrolla en $n-1$ iteraciones. La siguiente vez, i se ha incrementado a 1, por lo que el bucle interno (j) comienza en 2 y se procesa hasta $n-1$, es decir, se desarrolla en $n-2$ iteraciones. Y así sucesivamente: para la tercera iteración del bucle externo se obtienen $n-3$ iteraciones del interno, para la cuarta, $n-4$, etc. Para la última iteración del bucle externo, cuando el valor de i es $n-1$, el bucle interno (j) comienza en n y no se procesa, es decir, 0 iteraciones.

El número total de iteraciones del bucle interno es, pues, la suma [¡esto requiere justificación! ✍] de todos estos números anteriores de iteraciones, es decir, $(n-1)+(n-2)+(n-3)+\ldots+1+0$. ■

Actividad 19.23

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Observación 19.6.3.— La suma $(n-1)+(n-2)+(n-3)+\ldots+1+0$ es el $(n-1)$-ésimo número triangular[34], de expresión explícita $T_{n-1}=\dfrac{n\cdot(n-1)}{2}$.

Ejemplo 710

```
// subproceso que recibe el argumento n por valor
// y devuelve el número de iteraciones del bucle interno
SubProceso res <- f(n Por Valor)
    res <- 0 // inicialización del contador de iteraciones
    // tres iteraciones anidadas
    Para i0 Desde 1 Hasta n Con Paso 1 Hacer
        Para i1 Desde 1 Hasta i0 Con Paso 1 Hacer
            Para i2 Desde 1 Hasta i1 Con Paso 1 Hacer
                res <- res + 1 // incremento del contador de iteraciones
            FinPara
        FinPara
    FinPara
FinSubProceso

Proceso numdeiterbucleinterno
    Escribir "Introduzca un n.º entero positivo"
    Leer n
    Escribir "El n.º de iteraciones del bucle interno es ", f(n)
FinProceso
```

[CEOV 2020-2021, 2021-2022 (p.h.e.c.)].

Resolución.— Cada terna de valores de los índices i_0, i_1, i_2 es una selección no ordenada (debido a que i_0, i_1, i_2 son tales que $1\leq i_2\leq i_1\leq i_0\leq n$) con reemplazamiento (pues pueden tomar valores iguales) de 3 elementos del conjunto $\{1,2,\ldots,n\}$. El valor inicial de *res* es 0 y cada vez que los bucles se procesan con una terna de valores válidos de i_0, i_1, i_2, la variable *res* incrementa su valor en 1, correspondiendo cada procesamiento a una iteración del bucle interno. Por tanto, el número de iteraciones del bucle interno es el número de procesamientos de los bucles con una terna de valores válidos de i_0, i_1, i_2 y como cada terna de estos valores es una selección de las comentadas, el número de iteraciones buscado es $CR(n,3)$ (*cfr. supra* cuadro n.º 0 —teorema 19.45 (pág. 1191 de esta edición)—), esto es, $C(n+3-1,3)$, siendo 3 el número de bucles anidados. ■

[34] *Vid. The On-Line Encyclopedia of Integer Sequences*, sucesión A000217, https://oeis.org/A000217.

Ejemplo 711

```
// subproceso que recibe el argumento n por valor
// y devuelve el número de iteraciones del bucle interno
SubProceso res <- f(n Por Valor)
    res <- 0 // inicialización del contador de iteraciones
    // tres iteraciones anidadas
    Para i0 Desde 1 Hasta n Con Paso 1 Hacer
        Para i1 Desde i0 Hasta n Con Paso 1 Hacer
            Para i2 Desde i1 Hasta n Con Paso 1 Hacer
                res <- res + 1 // incremento del contador de iteraciones
            FinPara
        FinPara
    FinPara
FinSubProceso

Proceso numdeiterbucleinterno
    Escribir "Introduzca un n.º entero positivo"
    Leer n
    Escribir "El n.º de iteraciones del bucle interno es ", f(n)
FinProceso
```

[CEOV 2020-2021, 2021-2022 (p.h.e.c.)].

Resolución.— Análogo al anterior, sólo que considerando en este caso que ocurre que $1 \leq i_0 \leq i_1 \leq i_2 \leq n$, el resultado es $CR(n, 3) = C(n+3-1, 3)$, donde 3 es el número de bucles anidados. ■

Ejemplo 712

¿Qué ocurre con las dos últimas cuestiones en la situación general, esto es, si hubiese k bucles anidados?

[CEOV 2020-2021, 2021-2022 (p.h.e.c.)].

Resolución.— Pues que por lo comentado en las anteriores resoluciones, donde 3 era el número de bucles anidados, ahora, con k bucles anidados, el número de iteraciones del bucle interno es $CR(n, k) = C(n + k - 1, k)$. ■

Observación 19.6.4.— Por si quisiésemos visualizar lo que ocurre en el caso $n = 3$ con PSeInt.

```
SubProceso productorio <- factorial(n)
    productorio <- 1
    Para i Desde 2 Hasta n Con Paso 1 Hacer
        productorio <- productorio * i
    FinPara
FinSubProceso

SubProceso res <- coefbinomial(n,k)
    res <- factorial(n)/(factorial(k)*factorial(n-k))
FinSubProceso

// subproceso que recibe el argumento n por valor
// y devuelve el número de iteraciones del bucle interno
SubProceso res <- f(n Por Valor)
    res <- 0 // inicialización del contador de iteraciones
    // tres iteraciones anidadas
    Para i0 Desde 1 Hasta n Con Paso 1 Hacer
        Para i1 Desde i0 Hasta n Con Paso 1 Hacer
            Para i2 Desde i1 Hasta n Con Paso 1 Hacer
                res <- res + 1 // incremento del contador de iteraciones
            FinPara
        FinPara
    FinPara
FinSubProceso

Proceso numdeiterbucleinterno
    Escribir "Introduzca un n.º entero positivo"
    Leer n
    Escribir "N.º iter. bucle int. = ", f(n), "; CR(n,3) = ", coefbinomial(n+3-1,3)
FinProceso
```

Ejemplo 713

Como premio al esfuerzo por resolver el «problema de la semana», se decidió regalar exactamente siete libros a las personas más comprometidas, que resultaron ser tres. ¿De cuántas formas pudieron adjudicarse los libros si se resolvió que cada persona debía recibir al menos dos libros?

[EFO 17.1.2022:7]. *Cfr.* García, Hernández y Nevot [150], problema resuelto 5.26 (pág. 204).

Resolución.— Una de las personas, digamos P_0, recibirá tres libros y las otras dos, digamos P_1 y P_2, dos cada una. El suceso $S \rightleftharpoons$ «dado comenzar por una persona determinada [P_0], repartir los libros» se divide en tres fases:

S_0, adjudicación de tres libros a P_0, libros que pueden elegirse de $C(7,3) = 35$ formas (razonemos en el ámbito, por ejemplo, de la modelización II: objetos indistinguibles, tres marcas; recipientes distinguibles, los siete libros; aplicación inyectiva —no puede marcarse dos veces el mismo libro—), por lo que 35 es el número de formas posibles en que es posible realizar esta fase;

S_1, adjudicación de dos libros a P_1, fase que por un razonamiento análogo al anterior, es posible realizar de $C(7-3,2) = 6$ formas posibles;

S_2, adjudicación de dos libros a P_2, fase que por un razonamiento análogo al anterior, es posible realizar de $C(7-3-2,2) = 1$ formas posibles;

por lo que por el principio de la multiplicación, fijada la persona inicial, existen $\#S_0 \cdot \#S_1 \cdot \#S_2 = 35 \cdot 6 \cdot 1 = 210$ formas de adjudicarlos.

Como, en realidad, la persona inicial puede ser cualquiera de las tres, entonces, por el principio de adición [¡esto requiere justificación! ✍], el número de formas es $210 + 210 + 210 = 630$.

Solución.— De 630 formas. ∎

Actividad 19.24

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Observación 19.6.5.— Si hubiésemos interpretado del enunciado que sólo importase el número de libros que recibe cada persona, entonces si x_i designa el número de libros que recibe la persona i, el número de adjudicaciones posibles es igual al número de soluciones enteras de la ecuación $x_1+x_2+x_3 = 7$ tales que $(\forall i \in \{1,2,3\})(2 \leq x_i)$, que según el teorema 19.43 (pág. 1186 de esta edición)

es $CR(3,7-2\cdot 3) = CR(3,1) = C(3+1-1,1) = C(3,1) = 3$ (concretamente las adjudicaciones $\langle 3,2,2\rangle$, $\langle 2,3,2\rangle$ y $\langle 2,2,3\rangle$).

Ejemplo 714

Una ONG repartió 32 contenedores similares con paquetes de alimentos entre cinco poblados de forma que los dos más grandes recibieron, entre los dos, 23 contenedores. ¿De cuántas formas pudo hacerlo?

[EFO 17.1.2022:8]. *Cfr.* García, Hernández y Nevot [150], problema resuelto 5.33 (pág. 207).

Resolución.— Razonemos en el ámbito, por ejemplo, de la modelización II: los objetos son los contenedores, indistinguibles; los recipientes, los poblados, distinguibles; la aplicación puede ser de cualquier tipo, ya que no está sujeta a más restricción que a ser aplicación (función total), esto es, a que todos y cada uno de los objetos debe ser colocado en un solo recipiente (todos los contenedores deben ser repartidos, debiendo ir cada uno de ellos a no más de un poblado) (el orden de los objetos en los recipientes no influye en el recuento, ya que aquéllos, los contenedores, son indistinguibles).

Notemos lo extraño de este reparto, pues existe la posibilidad de que hasta dos poblados de los cinco no reciban ningún contenedor. En cualquier caso, subyace el principio de la multiplicación: sea el suceso $S \leftrightharpoons$ repartir 32 contenedores similares con paquetes de alimentos entre cinco poblados de forma que los dos más grandes reciban, entre los dos, 23 contenedores; la ocurrencia de S sucede en dos fases consecutivamente independientes: S_0, se lleva a cabo el reparto entre los dos poblados más grandes, cuestión que puede realizarse de $CR(2,23) = C(2+23-1,23) = 24$ formas; S_1, se reparte lo que queda entre el resto, cosa que puede hacerse de $CR(3,32-23) = C(3+9-1,9) = 55$ formas; entonces, por el principio de la multiplicación, el suceso S puede ocurrir de $\#S = \#S_0 \cdot \#S_1 = 24 \cdot 55 = 1320$ formas.

Solución.— El reparto pudo haberse efectuado de 1320 formas. ■

Ejemplo 715

En el primer millar de números enteros no negativos, esto es, desde 0 hasta 999, ambos incluidos; ¿qué hay más, números que tienen alguna cifra 1 o números que no la tienen?

Nota.— Resolvamos esta cuestión: I., incluyendo en nuestro razonamiento alguna —a nuestra elección— de las cuatro modelizaciones combinatorias, y II., interpretando el resultado de acuerdo con cada una de las demás modelizaciones que consideremos compatibles con la situación expuesta en la cuestión en estudio. Es importante para nuestra práctica que en cada una de las modelizaciones identifiquemos claramente cómo está representado cada número.

[EFE 25.6.2019:7], [EFO 27.5.2025:8], [EFE 18.6.2025:8].

Resolución.— Razonemos en el ámbito, por ejemplo, de la modelización II.

Pudiésemos contar el total de números enteros no negativos que contienen la cifra 1 o el total de los que no contienen la cifra 1. Decidimos contar estos últimos. Convenimos en que si el número tiene menos de tres cifras, le añadimos por la izquierda los ceros necesarios para que las tenga —por ejemplo, 3 será 003 y 23 será 023—, dicho de otro modo, en vez de trabajar con números decimales, lo haremos con palabras decimales (por lo que hablaremos de letras en vez de cifras).

Tras esta presentación, centrémonos ahora en resolver la cuestión según se exige. Elegimos la modelización II.

I. *Cálculo del recuento de acuerdo con la modelización II*.

Como problema de distribución, se trata de distribuir:

A. 3 objetos distinguibles (las distintas posiciones), en

B. 9 recipientes distinguibles (las distintas letras $\{0, 2, 3, \ldots, 9\}$),

C. no estando la correspondencia entre objetos y recipientes sujeta a más restricción que a ser aplicación (función total), esto es, a que todos y cada uno de los objetos debe ser colocado en un solo recipiente (en cada posición tiene que haber una letra, y sólo una) —pensemos que exigir inyectividad equivaldría a contar sólo palabras sin letras repetidas y exigir sobreyectividad equivaldría a contar sólo aquellas palabras que contuviesen todas las letras (lo cual es imposible al tratarse de palabras que representan números de como mucho tres cifras);

D. además, el orden de colocación de los objetos en los recipientes no importa —por ejemplo, 077, el 7 (recipiente) contiene las posiciones 2 y 3 (objetos), cuyo orden «dentro» de 7 da igual (notemos cómo las órdenes de formación «“7” en la posición “2” y “7” en la posición “3”» y «“7” en la posición “3” y “7” en la posición “2”» son equivalentes debido a la conmutatividad del conjuntor y por tanto, ambas representan a la misma palabra, a saber, 077).

En definitiva, cada palabra (y, por lo tanto, cada número) está representada por una distribución simple de 3 objetos distinguibles en 9 recipientes distinguibles, no estando la correspondencia entre objetos y recipientes sujeta a más restricción que a ser aplicación y siendo la distribución no ordenada.

En estas condiciones, por un teorema conocido sobre distribuciones no ordenadas (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—), el número total buscado es:

$$VR(9,3) = 9^3 = 729.$$

II. *Interpretación del resultado de acuerdo con cada una de las demás modelizaciones compatibles con la situación expuesta*.

A. *Interpretación de acuerdo con la modelización I*.

Cada palabra (y, por lo tanto, cada número) está representada por una selección simple (muestra) ordenada de 3 objetos (las letras que irán en las tres posiciones en la palabra) de un total de 9 objetos distinguibles (las letras $\{0, 2, 3, \ldots, 9\}$), selección que es ordenada (pues el orden de los objetos en la muestra importa para distinguir muestras: $\langle 0, 7, 3\rangle \neq \langle 3, 7, 0\rangle$, ya que dicho orden es el orden de colocación de las letras elegidas en las posiciones 0, 1 y 2 de la palabra) y siendo la reposición de objetos con reemplazamiento (para poder representar palabras con letras repetidas, por ejemplo, la muestra $\langle 4, 4, 0\rangle$ representa la palabra 440).

B. *Interpretación de acuerdo con la modelización III*.

Cada palabra (y, por lo tanto, cada número) está representada por una partición simple ordenada (una tupla) de un conjunto de 3 elementos distinguibles, $\{0, 1, 2\}$ (las tres posiciones en la palabra) en 9 subconjuntos no ordenados, pudiendo ser algunos vacíos y algunos no unitarios. Por ejemplo, la partición $\langle\{2\}, \emptyset, \emptyset, \{0, 1\}, \emptyset, \emptyset, \emptyset, \emptyset, \emptyset\rangle$ representa la palabra 440. Apreciamos: 0., que puede haber subconjuntos vacíos y no unitarios; 1., que se trata de subconjuntos no ordenados por el mismo motivo que discutimos en I.D (pág. 1266 de esta edición), sus elementos indican posiciones de una misma letra (da igual decir que 4 está en las posiciones 0 y 1 que decir que está en las posiciones 1 y 0), y 2., que la partición es ordenada (el orden de los subconjuntos en la partición importa para distinguir particiones) ya que las posiciones en la partición representan ordenadamente las letras $\{0, 2, 3, \ldots, 9\}$.

C. *Interpretación de acuerdo con la modelización IV*.

Las *modelizaciones compatibles* son la I, II y III. La IV no lo es porque al representar un entero positivo k como la suma de k unos, estos unos, indistinguibles, son los correspondientes a los objetos, que, por tanto, deberían ser indistinguibles, pero en la situación en estudio,

el lugar de estos objetos lo ocupan letras, que son distinguibles (esto se refleja en el tercer diccionario intermodal, *cfr. supra* cuadro n.º 7—teorema 19.58 (pág. 1212 de esta edición)—).

Solución.— En el primer millar de números enteros no negativos son más los que no contienen la cifra 1 (729 frente a 271[$= 1000 - 729$]). ■

Observación 19.6.6.— Pudiésemos pensar en **otra vía** de resolución mediante el principio de la multiplicación. Sea el suceso $S \leftrightharpoons$ construcción de una palabra decimal de tres letras que no contiene la letra 1, y las fases consecutivamente independientes $S_0 \leftrightharpoons$ construcción de la letra en la posición cero con letras diferentes a 1, $S_1 \leftrightharpoons$ construcción de la letra en la posición uno con letras diferentes a 1, y $S_2 \leftrightharpoons$ construcción de la letra en la posición dos con letras diferentes a 1. Cada una de estas fases puede realizarse de 9 formas, tantas como letras hay en $\{0, 2, 3, \ldots, 9\}$. En definitiva, $\#S = \#S_0 \cdot \#S_1 \cdot \#S_2 = 9 \cdot 9 \cdot 9 = 729$. Observemos que pudiésemos hacer partícipe a la modelización; por ejemplo, según la modelización I, una realización de cualquiera de las fases no es más que una selección simple sin reemplazamiento de una letra de un conjunto de 9 letras distinguibles (selección ordenada o no, es indiferente por seleccionarse una única letra), por lo que el número de formas de realizar cualquiera de las fases no sería otra cosa que el número de selecciones simples sin reemplazamiento de una letra de un conjunto de 9 letras distinguibles, esto es, [selección ordenada] $V(9,1) = 9 = C(9,1)$ [selección no ordenada].

Ejemplo 716

Se quiere poner un examen de puntuación máxima doce puntos con cuatro cuestiones de tal manera que cada una puntúe como mínimo dos puntos. Encontremos el número total de formas de crear tal hoja de examen.

[EFO 3.6.2019:7].

Resolución.— La situación es equivalente a tener que encontrar el número de soluciones enteras no negativas de $x_1 + x_2 + x_3 + x_4 = 12$ tales que con las restricciones $(\forall i \in \{1, 2, 3, 4\})(2 \leq x_i)$.

Razonemos en el ámbito, por ejemplo, de la modelización II. Se trata de distribuir 12 objetos indistinguibles (12 es suma de doce 1 indistinguibles) en 4 recipientes distinguibles (las 4 incógnitas —cada una representando una de las 4 cuestiones—); el orden de colocación de los objetos en los recipientes no importa (la colocación de k objetos en el recipiente x_i modeliza el valor de la variable, $x_i = k$ —esto es la suma de k unos, dando igual el orden de los unos—, valor que representa la puntuación asignada a la pregunta i).

Si se satisfacen primero las restricciones, se deben distribuir dos objetos en cada recipiente, esto es, un total de $2 \cdot 4$ objetos indistinguibles en 4 recipientes distinguibles, para lo cual sólo hay una manera de hacerlo. Pensemos, por ejemplo, en elegir 2 unos de los 12 (sólo una forma por ser los unos indistinguibles) y colocar cada una de esas parejas de unos en cada caja consecutivamente,

entonces, por el principio de la multiplicación, $1 \cdot 1 \cdot 1 \cdot 1 = 1$; tras ello, quedan $k = 4(= 12 - 2 \cdot 4)$ objetos indistinguibles por distribuir en $n = 4$ recipientes distinguibles; de este modo, la aplicación subyacente no está sujeta a ninguna restricción (si se exigiera inyectividad, las variables no podrían valer más de tres —parten de un valor igual a 2— y si se exigiese sobreyectividad no podrían valer 2 —cuando sí es un valor posible—).

En definitiva, por un teorema conocido (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—), el número total buscado es $CR(n, k)$, esto es,

$$\begin{aligned} CR(4, 12 - 2 \cdot 4) &= CR(4, 4) \\ &= C(4 + 4 - 1, 4) \\ &= C(7, 4) \\ &= \frac{7!}{3! \cdot 4!} \\ &= 35. \end{aligned}$$ ■

Observación 19.6.7.— **Otra vía** de resolución (participando igualmente la modelización II) habría sido repartir 1 punto a cada cuestión al principio (lo cual sólo puede hacerse de una forma —razonado anteriormente—) y pensar en el nuevo problema que queda: repartir $k = 8$ objetos indistinguibles (los 8 unos restantes) en $n = 4$ recipientes distinguibles (las 4 cuestiones), sujeto ahora a la condición de que cada una puntúe como mínimo un punto (esto es, la aplicación subyacente es sobreyectiva); como no importa el orden de colocación de los objetos en los recipientes (razonado anteriormente), se tiene, por un teorema conocido (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—) que la solución es $CR(n, k - n)$, esto es, $CR(4, 8 - 4) = CR(4, 4) = 35$.

Ejemplo 717

Se están estudiando las posibles distribuciones de p personas en las q filas de sillas de un aula de examen ($q \leq p$). Supongamos que la capacidad de cada fila es ilimitada.

0. ¿Cuántas disposiciones posibles de personas hay si
   a. no hay filas vacías?
   b. en la segunda fila hay exactamente s personas ($s \leq p$)?
   c. en las primeras r filas hay $a_1, a_2, \ldots, a_r$ personas, respectivamente ($a_1 + a_2 + \cdots + a_r \leq p$)?
   d. en la fila iésima se encuentran no menos de a_i personas ($\forall i \in \{1, 2, \ldots, q\}$) ($a_1 + a_2 + \cdots + a_q \leq p$)?
1. Calculemos los resultados anteriores para los valores $p = 7$, $q = 3$, $s = 2$, $r = 2$, $a_1 = 1$, $a_2 = 2$ y $a_3 = 3$.

[EFE 25.6.2019:5].

Resolución.— Razonemos en el ámbito, por ejemplo, de la modelización II.

0. Notemos que en todos los apartados usamos la igualdad:

$$CR(n,k) = C(n+k-1,k),$$

siendo $CR(n,k)$ y $C(n,k)$ las combinaciones con y sin repetición, respectivamente, de k elementos de n dados. Por otro lado, en la modelización como problemas de distribución notamos por k el número de objetos y por n el de recipientes. Por llevarlo a un terreno trabajado, observemos que todas las situaciones son equivalentes a tener que encontrar el número de soluciones enteras no negativas de $x_1 + x_2 + \cdots + x_q = p$, con ciertas restricciones en cada caso:

I. los «objetos» a distribuir son las personas, indistinguibles porque no las tenemos en cuenta individualmente, pues sólo nos interesa su número en cada fila (en la ecuación, el valor de la incógnita correspondiente);

II. los «recipientes» son las filas de sillas, distinguibles al interesarnos el número de personas sentadas en ellas (cada una de las q incógnitas representa una de las q filas de sillas);

III. 0. en los *apartados* 0.*a*, 0.*b* y 0.*c*, la *correspondencia entre objetos y recipientes* no está sujeta a más restricción que a ser aplicación (función total), esto es, a que todos y cada uno de los objetos debe ser colocado en un solo recipiente (deben sentarse todas las personas y cada una en una sola fila de sillas) —pensemos que exigir inyectividad equivaldría a exigir que sólo pudiese sentarse una persona por fila (0 y 1 como únicos valores posibles de las variables) y exigir sobreyectividad equivaldría a exigir que en cada fila se sentase al menos una persona (todos los valores de las variables mayores o iguales a 1);

I. es precisamente esto último, la sobreyectividad, lo exigido por el *apartado* 0.*a*, esto es, $\forall i \in \{1,2,\ldots,p\}, x_i \geq 1$;

IV. el *orden de colocación* de los objetos en los recipientes no importa (la colocación de h objetos en el recipiente x_i modeliza el valor de la variable, $x_i = h$ [esto es, el recuento de h personas, dando igual el orden en que se sienten las personas al interesar sólo su número], valor que representa el número de personas asignado a la fila i).

En estas condiciones, se tiene que:

0.a. Se trata de distribuir,

I. sin importar el orden de colocación de los objetos en cada recipiente (distribución no ordenada),

II. p objetos indistinguibles (todos) en

III. q recipientes distinguibles (todos),

IV. con la condición de que en cada recipiente haya al menos un objeto (aplicación sobreyectiva).

Por un teorema conocido sobre distribuciones no ordenadas (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—), siendo $n = q$ y $k = p$, el número total buscado es:

$$\begin{aligned} CR(q, p-q) &= C(q + (p-q) - 1, p-q) \\ &= \binom{p-1}{p-q} \\ &= \frac{(p-1)!}{(p-q)! \cdot (q-1)!} \end{aligned}$$

0.b. Una vez colocados s objetos en el segundo recipiente, satisfecha así la restricción, se trata de distribuir,

I. sin importar el orden de colocación de los objetos en cada recipiente (distribución no ordenada),

II. $p - s$ objetos indistinguibles(todos menos los s del recipiente 2.º) en

III. $q - 1$ recipientes distinguibles (todos menos el 2.º),

IV. sin condiciones (aplicación cualquiera).

Por un teorema conocido sobre distribuciones no ordenadas (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—), siendo $n = q - 1$ y $k = p - s$, el número total buscado es:

$$\begin{aligned} CR(q-1, p-s) &= C((q-1) + (p-s) - 1, p-s) \\ &= \binom{p+q-s-2}{p-s} \\ &= \frac{(p+q-s-2)!}{(p-s)! \cdot (q-2)!} \end{aligned}$$

0.c. Una vez distribuidos $\sum_{i=1}^{r} a_i$ objetos en los r primeros recipientes, satisfecha así la restricción, se trata de distribuir,

I. sin importar el orden de colocación de los objetos en cada recipiente (distribución no ordenada),

II. $p - \sum_{i=1}^{r} a_i$ objetos indistinguibles (todos menos los ya distribuidos),

III. en $q - r$ recipientes distinguibles (todos menos los r primeros),

IV. sin condiciones (aplicación cualquiera).

Por un teorema conocido sobre distribuciones no ordenadas (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—), siendo $n = q - r$ y $k = p - \sum_{i=1}^{r} a_i$, el número total buscado es:

$$\begin{aligned} CR(q-r, p - \sum_{i=1}^{r} a_i) &= \binom{(q-r) + (p - \sum_{i=1}^{r} a_i) - 1}{p - \sum_{i=1}^{r} a_i} \\ &= \binom{q - r + p - \sum_{i=1}^{r} a_i - 1}{p - \sum_{i=1}^{r} a_i} \\ &= \frac{(q - r + p - \sum_{i=1}^{r} a_i - 1)!}{(p - \sum_{i=1}^{r} a_i)! \cdot (q - r - 1)!} \end{aligned}$$

0.d. Una vez distribuidos $\sum_{i=1}^{q} a_i$ objetos en los q recipientes, satisfecha así la restricción, se trata de distribuir,

I. sin importar el orden de colocación de los objetos en cada recipiente (distribución no ordenada),

II. $p - \sum_{i=1}^{q} a_i$ objetos indistinguibles (todos menos los ya distribuidos),

III. en q recipientes distinguibles (todos),

IV. sin condiciones (aplicación cualquiera).

Por un teorema conocido sobre distribuciones no ordenadas (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—), siendo $n = q$ y $k = p - \sum_{i=1}^{q} a_i$, el número total buscado es:

$$\begin{aligned} CR(q, p - \sum_{i=1}^{q} a_i) &= \binom{q + (p - \sum_{i=1}^{q} a_i) - 1}{p - \sum_{i=1}^{q} a_i} \\ &= \binom{q + p - \sum_{i=1}^{q} a_i - 1}{p - \sum_{i=1}^{q} a_i} \\ &= \frac{(q + p - \sum_{i=1}^{q} a_i - 1)!}{(p - \sum_{i=1}^{q} a_i)! \cdot (q - 1)!} \end{aligned}$$

1. Siendo $p = 7$, $q = 3$, $s = 2$, $r = 2$, $a_1 = 1$, $a_2 = 2$, y $a_3 = 3$, se tiene que los resultados son:

a. $\dfrac{(7-1)!}{(7-3)! \cdot (3-1)!} = 15;$

b. $\dfrac{(7+3-2-2)!}{(7-2)! \cdot (3-2)!} = 6;$

c. $\dfrac{(3-2+7-(1+2)-1)!}{(7-(1+2))! \cdot (3-2-1)!} = 1;$

d. $\dfrac{(3+7-(1+2+3)-1)!}{(7-(1+2+3))! \cdot (3-1)!} = 3.$ 

Ejemplo 718

Supongamos que queremos situar k libros distintos en los estantes de una estantería de n estantes. Para simplificar, supongamos que todos los libros pudieran coger en uno cualquiera de los estantes y que sólo nos interesa la situación relativa de los libros entre ellos. ¿De cuántas formas es posible colocar los libros si queremos poner al menos uno en cada estante?

[SEL 11:4]. *Cfr.* BOGART [219]: problema 123 (pág. 61-62).

Resolución.—

Respuesta muy breve.— Como sabemos, la asignación de qué libros van a qué estantes es una aplicación de los libros a los estantes. Como de cada estante se requiere que consiga al menos un libro, esta aplicación es sobreyectiva. Como importa el orden en que los estantes reciben sus libros, entonces es una distribución ordenada de k objetos distinguibles (los k libros distintos) a n recipientes distinguibles (los n estantes). Según el cuadro n.º 2b, el número de distribuciones es igual a $P(n) \cdot L(k, n) = k! \cdot C(k-1, n-1)$.

Respuesta larga y autojustificada.— Primero, analicemos de cuántas maneras podemos colocar todos los libros sin tener en cuenta el requisito de que debe haber al menos uno en cada estante.

Hagámonos algunas preguntas y respondámoslas.

- ¿En cuántos lugares podemos colocar el primer libro?

  Hay n lugares donde podemos colocar el primer libro (en cualquiera de los n estantes).

- Cuando colocamos el segundo libro, si decidimos colocarlo en el estante que tiene el primer libro, ¿importa si lo colocamos a la izquierda o a la derecha del primer libro?

  Del enunciado (son libros distintos) y de nuestra manera de entender nuestra lengua, si no nos dicen nada, importa, no es lo mismo la disposición (libro A, libro B) que (libro B, libro A), así que sí, sí importa.

- ¿En cuántos lugares podemos colocar el segundo libro?

  Hay $n+1$ lugares donde podemos colocar el segundo libro, porque en la estantería que tiene el primer libro, pudiésemos poner el segundo libro a la izquierda o a la derecha del primero ($n-1$ estantes libres y dos posiciones en el que está el primero).

- Una vez que tenemos $i-1$ libros colocados, si queremos colocar el libro iésimo en una estantería que ya tiene algunos libros, ¿deslizarlo a la izquierda de todos los libros que ya hay es diferente a colocarlo a la derecha de todos los libros que ya hay y diferente a colocarlo entre dos libros que ya hay?

A ver, ¿no es esta situación una extensión de la pregunta sobre el segundo libro a izquierda o derecha del primero? Así que la respuesta es sí, todos esos casos son diferentes.

- ¿De cuántas formas podemos colocar el libro iésimo en la estantería?

  Hay $n + i - 1$ lugares donde podemos colocar el libro iésimo, esto es así porque una vez que tenemos $i - 1$ libros en los estantes, el libro iésimo podría ir en cualquier estante a la izquierda de todos los libros que hay en él, si los hubiese, estos son n lugares, o podría ir a la derecha inmediata de cualquier libro que estuviera ya allí, estos son otros $i - 1$ lugares (hay $i - 1$ libros colocados).

- ¿De cuántas formas podemos colocar todos los libros?

  Por el principio de la multiplicación [¡esto requiere justificación! ✍], el número de formas de colocar todos los libros (sin el requisito de que debe haber al menos uno en cada estante) —usando la notación de DIJKSTRA[35]— es $\langle \Pi i : 1 \leq i < k+1 : n+i-1 \rangle$, esto es, el producto $(n+1-1) \cdot (n+2-1) \cdot \cdots \cdot (n+k-1)$ (observemos que este producto es el factorial ascendente kaésimo de n).

- Finalmente, suponiendo que cada estante recibe al menos un libro, ¿de cuántas formas podemos colocar todos los libros?

  Podemos elegir n libros de los k libros de $C(k, n)$ formas [¡esto requiere justificación! ✍], y asignarlos a los n lugares de los estantes de $n!$ formas [¡esto requiere justificación! ✍], proporcionándonos así, por el principio de la multiplicación, $k!/(k-n)!$ formas de poner un libro en cada estante [¡esto requiere justificación! ✍]. Ahora, dejando estos libros en el extremo izquierdo de cada estante (cosa que podemos hacer de $C(k-n, k-n) = 1$ formas), podemos colocar los $k - n$ libros restantes de

  $$\begin{aligned} \langle \Pi i : 1 \leq i < k-n+1 : n+i-1 \rangle &= (n+(k-n)-1)!/(n-1)! \\ &= (k-1)!/(n-1)! \end{aligned}$$

  formas.

  Por lo tanto, por el principio de la multiplicación [¡esto requiere justificación! ✍], hay

  $$\begin{aligned} (k!/(k-n)!) \cdot ((k-1)!/(n-1)!) &= k! \cdot C(k-1, n-1) \\ &= P(n) \cdot L(k, n) \end{aligned}$$

  formas de colocar los libros[36]. ■

[35] *Vid. supra* § 5.6.2 (pág. 429 de esta edición).

[36] Tranquila y reflexivamente, procuremos justificar todos los pasos que requieren ser justificados, es una buena práctica, además de ser necesario y conveniente; observemos que en esta última parte hay un principio de la multiplicación «externo» con dos fases, cada una de éstas calculado su número de formas de realización con un principio de la multiplicación, también con dos fases

§ 19.7 Propuesta de más actividades

Actividad 19.25

Apliquemos el principio de los cajones (generalizado o no) de Dirichlet para demostrar que en una reunión a la que asisten n personas y se saludan todas entre sí una vez, entonces al menos dos personas han saludado al mismo número de personas.

[SEL 9:2b]. *Cfr.* Franco, Espinel y Almeida [214]: ejercicio 3.14 (págs. 49–50).

Actividad 19.26

En una asamblea se puede elegir, de 506 maneras distintas, de entre todas las personas asistentes, dos puestos, la coordinación y la secretaría. ¿Cuántas personas asisten a dicha asamblea?

[SEL 9:4]. *Cfr.* Franco, Espinel y Almeida [214]: ejercicio 4.33 (pág. 88).

Actividad 19.27

¿De cuántas formas pueden distribuirse siete personas en tres habitaciones distintas, una con tres camas y dos con dos camas?

[SEL 10:1]. *Cfr.* Franco, Espinel y Almeida [214]: ejercicio 4.8 (pág. 82).

Actividad 19.28

¿De cuántas formas pueden ordenarse las 27 letras del alfabeto español de forma que:

0. las vocales aparezcan juntas?
1. las letras A y B no aparezcan juntas?

[SEL 10:2]. *Cfr.* Franco, Espinel y Almeida [214]: ejercicio 4.17 (pág. 84).

Actividad 19.29

Calculemos de cuántas formas se pueden situar ocho torres en un tablero de ajedrez 8×8, de modo que ninguna sea amenazada por otra.

[SEL 10:3]. *Cfr.* Franco, Espinel y Almeida [214]: ejercicio 3.7 (pág. 36).

Actividad 19.30

Sean ocho bolas numeradas del 0 al 7, las cuatro primeras blancas y las cuatro restantes rojas.

0. ¿De cuántas formas pueden ordenarse dichas ocho bolas, de modo que los dos colores queden alternados?
1. ¿Y si las bolas 3 y 4 han de quedar juntas?

[SEL 10:4]. *Cfr.* Ferrando y Gregory [156]: ejercicio 5.10 (pág. 174).

Actividad 19.31

Una empresa proveedora de cáterin está preparando tres bolsas de almuerzos para excursionistas. La empresa tiene nueve emparedados diferentes.

0. ¿De cuántas maneras se pueden distribuir estos nueve emparedados en tres bolsas de almuerzo idénticas de forma que en cada bolsa haya al menos uno?
1. ¿Y si las bolsas son distintas?

[SEL 11:6]. *Cfr.* Bogart [219]: problema 146 (pág. 67).

Actividad 19.32

¿De cuántas formas pueden distribuirse tres premios entre dos personas si

0. los premios son indistinguibles y
   a. cada persona puede conseguir como mucho un premio?
   b. cada persona puede conseguir cualquier número de premios?
   c. cada persona ha de conseguir al menos un premio?
1. los premios son distinguibles y
   a. cada persona puede conseguir como mucho un premio?
   b. cada persona puede conseguir cualquier número de premios?
   c. cada persona ha de conseguir al menos un premio?

[EFEC 25.6.2019:5].

Actividad 19.33

¿Cuántas soluciones enteras tiene la ecuación

$$x_1 + x_2 + x_3 + x_4 = 25,$$

siendo $\forall i \in \{1, 2, 3, 4\}, x_i \geq -2$?

[EFEC 25.6.2019:7].

Actividad 19.34

¿Cuántas soluciones enteras no negativas tiene la ecuación $x_1 + x_2 + x_3 + x_4 + x_5 = 21$, tales que x_1, x_2, x_3, x_4 y x_5 satisfacen:

0. $x_1 \geq 1$?;
1. $x_i \geq 2$, para $i \in \{1, 2, 3, 4, 5\}$?;
2. $0 \leq x_1 \leq 10$?

[EFO 24.5.2018:6], [SEL 11:5]. *Cfr.* Franco, Espinel y Almeida [214]: ejercicio 7.10 (pág. 142).

Actividad 19.35

Hagamos el ejemplo 703 (pág. 1252 de esta edición) suponiendo que los diez libros son distintos.

Con miras a su resolución.— Por ejemplo, el apartado 1. Por el principio de multiplicación, el producto de: $C(10, 4)$ [selección no ordenada sin reposición de cuatro libros de diez distintos] por $P(4)$ (por ejemplo, por definición de permutación) (o si se exigiese modelización, $P(4) \cdot S(4, 4)$ [distribución no ordenada de los cuatro libros distintos en los cuatro estantes distintos con un libro en cada estante (aplicación sobreyectiva), o $P(4)$ [igual, con aplicación biyectiva, por ser $n = k$]) por $P(10-4) \cdot CR(4, 10-4)$ [distribución ordenada de 10-4 libros distintos en 4 estantes distintos). Notemos que si comparamos con la resolución para libros indistinguibles dada en el ejemplo 703 (pág. 1252 de esta edición), $CR(4, 10-4)$ ha de multiplicarse aquí por $C(10, 4) \cdot P(4)$ (lo aportado por la distinguibilidad de los cuatro libros) y por $P(10-4)$ (lo aportado por la distinguibilidad de los otros $10-4$ libros). Por cierto, una respuesta más corta es $P(4) \cdot L(10, 4)$, esto es, $P(10) \cdot C(10-1, 4-1)$ —*cfr. supra* ejemplo 718 (pág. 1273 de esta edición)—.

Actividad 19.36

Tres personas viajan en una guagua (como ellas llaman al autobús) que tiene siete paradas. ¿De cuántas maneras pueden apearse en los siguientes casos?

0. Si a lo sumo baja una persona por parada,
   a. pudiendo distinguirse las personas entre sí,
   b. no pudiendo distinguirse las personas entre sí (por ejemplo, llevan disfraces idénticos);
1. sin restricciones, pero
   a. pudiendo distinguirse las personas entre sí,
   b. no pudiendo distinguirse las personas entre sí.

[EFO 24.5.2018:5].

Actividad 19.37

¿Cuántos números en $\{1, 2, 3, \ldots, 100\,000\}$ satisfacen que la suma de sus cifras es 7?

[SEL 10:6]. *Cfr.* Ross y Wright [157]: ejemplo 11 (pág. 217).

Actividad 19.38

[(Números de Catalan)] ¿De cuántas maneras pudiésemos cubrir una forma escalonada de altura n con n rectángulos de tamaños variables?*

---

* Como punto de comienzo, *vid. v. gr.* https://www.numbersaplenty.com/set/Catalan_number/; por otra parte, el artículo en la Wikipedia en inglés (https://en.wikipedia.org/wiki/Catalan_number) y el correspondiente en la OEIS (https://oeis.org/A000108) incluyen un buen número de interpretaciones alternativas.

§ 19.8 Muestra de ejemplos finales

Ejemplo 719

Imaginemos ahora que para aumentar la seguridad de la red en línea de dieciocho computadores del ejemplo 608 (pág. 1109 de esta edición), por ejemplo, para evitar situaciones de propagación de programas malignos, se desea segmentarla en cuatro subredes (espacios de red más pequeños) en línea de como mínimo una tríada de computadores cada una. ¿De cuántas maneras puede llevarse esto a cabo?

[EFO 12.6.2020:3a (p.h.e.c.)].

Resolución.— Sea x_i el número de computadores pertenecientes a la subred r_i, entonces, el número de maneras de llevar a cabo dicha segmentación es el número de soluciones enteras de la ecuación

$$x_1 + x_2 + x_3 + x_4 = 18, \text{ siendo } \forall i \in \{1, 2, 3\}, 3 \leq x_i. \tag{19.5}$$

Sabemos por el teorema 19.43 (pág. 1186 de esta edición) que el número de soluciones enteras de $x_1 + x_2 + \cdots + x_n = k$, siendo $\forall i \in \{1, 2, \ldots, n\}, 0 \leq m \leq x_i$, con $m \cdot n \leq k$, es $CR(n, k - m \cdot n)$.

En el caso que nos ocupa, $n = 4$, $k = 18$, $m = 3$ y se satisface que $3 \cdot 4 < 18$. Por tanto, el número de soluciones enteras de (19.5) con $3 \leq x_i$ ($\forall i \in \{1, 2, 3\}$) es

$$CR(4, 18 - 3 \cdot 4) = CR(4, 6) = C(4 + 6 - 1, 6) = \binom{9}{6} = 84.$$

Solución.— La segmentación en subredes planteada puede realizarse de 84 maneras. ■

Observación 19.8.0.— Pudiésemos utilizar el artefacto en línea SageMath[37] y el siguiente programita en lenguaje Sage,

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
Compositions(18,length=4,min\_part=3).list()
```

para obtener las 84 soluciones de (19.5) y, por simple curiosidad, con

```
binomial(9,6)
```

calculamos el valor del coeficiente binomial.

Ejemplo 720

Continuando con el ejemplo anterior, se prevé que si ocurre un fallo generalizado, como en el ejemplo 608 (pág. 1109 de esta edición), no podrá contarse con exactamente seis de los computadores de los de mayor potencia (aunque no se sabe de cuáles se trataría), entonces, ¿de cuántas maneras puede llevarse a término la segmentación en subredes planteada si, como hemos dicho, vamos a estar obligados a prescindir de seis computadores de los de mayor potencia sin saber de cuáles se trata?

[EFO 12.6.2020:3b (p.h.e.c.)].

Resolución.— De cuántas formas se prescinde de los seis computadores de los de mayor potencia al no saber de cuáles se trata, será de cuántas formas pueden disponerse fuera de las subredes manteniendo sus conexiones originales al *bus*, en otras palabras, cuántos hay en los huecos entre subredes,

$$\square + x_1 + \square + x_2 + \square + x_3 + \square + x_4 + \square = 18; \tag{19.6}$$

notando por z_i al número de computadores en el hueco i,

$$z_0 + x_1 + z_1 + x_2 + z_2 + x_3 + z_3 + x_4 + z_4 = 18. \tag{19.7}$$

Observemos que como según el ejemplo 608 (pág. 1109 de esta edición), sólo se prevé que los que fallen estén entre los de mayor potencia, Litty sigue activo en el último lugar, y por tanto, de seguro que es el último de la cuarta subred, por lo que $z_4 = 0$. Esto hace que el número de computadores a distribuir en los huecos, manteniendo sus conexiones originales, son $11 = 18 - 6 - 1$ (este «1» es Litty).

Así, por un lado, se tiene

$$x_1 + x_2 + x_3 + x_4 = 11, \text{ siendo } \forall i \in \{1, 2, 3\}, 3 \leq x_i, \text{ y } 2 \leq x_4, \tag{19.8}$$

---

[37] *Cfr. supra* § 11 (pág. cii de esta edición).

que transformándola en una ecuación sujeta a la condición de no negatividad de sus variables, esto es, haciendo el cambio de variable $\forall i \in \{1, 2, 3\}$, $y_i = x_i - 3$, $y_4 = x_4 - 2$, para tener entonces, $\forall i \in \{1, 2, 3\}$,

$$\begin{aligned} x_i \geq 3 &\leftrightarrow x_i - 3 \geq 3 - 3 \\ &\leftrightarrow y_i \geq 0, \end{aligned}$$

y para $i = 4$,

$$\begin{aligned} x_4 \geq 2 &\leftrightarrow x_4 - 2 \geq 2 - 2 \\ &\leftrightarrow y_4 \geq 0, \end{aligned}$$

y así, de (19.8),

$$(x_1 - 3) + (x_2 - 3) + (x_3 - 3) + (x_4 - 2) = 11 - (3 \cdot 3 + 2) = 0,$$

por lo que (19.8) se ha transformado en

$$y_1 + y_2 + y_3 + y_4 = 0, \tag{19.9}$$

cuyo número de soluciones enteras no negativas es $CR(4, 0) = C(4 + 0 - 1, 0) = C(3, 0) = 1$ (*cfr. supra* teorema 19.43 [pág. 1186 de esta edición]); en efecto, al estar los computadores conectados en línea, sólo es posible una segmentación en cuatro subredes de tres computadores cada una, correspondiente a la solución $(y_1, y_2, y_3, y_4) = (0, 0, 0, 0)$ de (19.9), esto es, a la solución $(x_1, x_2, x_3, x_4) = (3, 3, 3, 2)$ de (19.8); dos ejemplos de tal segmentación son

$$\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{10, 11, \text{Litty}\},$$

y

$$\{1, 2, 3\}, \{5, 6, 7\}, \{10, 11, 12\}, \{16, 17, \text{Litty}\}.$$

Por otro lado, como mantenemos las conexiones originales al *bus*, razonando en el ámbito de la modelización II, cada distribución de los seis computadores que fallan en los cuatro «huecos» entre subredes corresponde a una distribución de seis objetos indistinguibles en cuatro recipientes distinguibles $z_0, z_1, \ldots$, distribución que es no ordenada (el orden de los computadores en los huecos no importa) y que no está sujeta a restricción alguna sobre la situación de los recipientes con respecto a los objetos (restricciones como si puede quedar alguno vacío, si no pueden contener más de un objeto, etc.). El número total de distribuciones es $CR(4, 6) = C(6 + 4 - 1, 4 - 1) = C(9, 3) = 84$ (*cfr. supra* cuadro n.º 2.a —teorema 19.47 (pág. 1198 de esta edición)—). Notemos que cada distribución es una solución entera de

$$z_0 + z_1 + z_2 + z_3 = 6, \text{ siendo } \forall i \in \{0, 1, 2, 3\}, 0 \leq z_i. \tag{19.10}$$

Tenemos, pues, por un lado, el conjunto S_1 de soluciones de 19.8 y por otro, el conjunto S_2 de soluciones de 19.10; entonces, por el principio de la multiplicación (*cfr. supra* § 19.1.1 [pág. 1138 de esta edición]), el número de soluciones del sistema

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = 11, \\ z_0 + z_1 + z_2 + z_3 = 6, \\ x_i \geq 3 \, (\forall i \in \{1, 2, 3\}), \\ x_4 \geq 2, \\ z_i \geq 0 \, (\forall i \in \{0, 1, 2, 3\}), \end{cases} \tag{19.11}$$

esto es, el cardinal del conjunto $S_1 \times S_2$, es $CR(4, 0) \cdot CR(4, 6) = 1 \cdot 84 = 84$.

Así, un par de ejemplos de soluciones particulares del sistema (19.11) son

$$(z_0, x_1, z_1, x_2, z_2, x_3, z_3, x_4) = (0, 3, 0, 3, 0, 3, 6, 2),$$

correspondiente a la segmentación en subredes

$$\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{10, 11, \text{Litty}\},$$

habiendo fallado los computadores n.º 12, 13, 14, 15, 16 y 17, y

$$(z_0, x_1, z_1, x_2, z_2, x_3, z_3, x_4) = (0, 3, 1, 3, 2, 3, 3, 2),$$

correspondiente a la segmentación en subredes

$$\{1, 2, 3\}, \{5, 6, 7\}, \{10, 11, 12\}, \{16, 17, \text{Litty}\},$$

habiendo fallado los computadores n.º 4, 8, 9, 13, 14 y 15.

Solución.— La segmentación en subredes planteada puede realizarse de 84 maneras. ■

Observación 19.8.1.— Pudiésemos utilizar el artefacto en línea SageMath[38] y el siguiente programita en lenguaje Sage,

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
Compositions(6,length=4,min\_part=0).list()
```

para obtener las 84 soluciones de (19.10).

[38] *Cfr. supra* § 11 (pág. cii de esta edición).

Ejemplo 721

De una colección de computadores (distinguibles), son 46 los que han superado 3 pruebas de rendimiento que se aprueban con calificaciones A, B o C. Demostremos que al menos 5 de esos 46 computadores han obtenido el mismo conjunto de calificaciones.

[EFE 14.7.2020:3a (p.h.e.c.)].

Resolución.— El enunciado habla de «conjunto» de calificaciones, por lo que da a entender que si un computador hubiese obtenido A en la prueba inicial, B en la intermedia y A en la final y otro computador, A en la inicial, A en la intermedia y B en la final, habrían obtenido el mismo conjunto de calificaciones —en realidad, habrían obtenido el multiconjunto $\{\{A, A, B\}\}$ (cuyo conjunto subyacente es $S = \{A, B, C\}$)—. De hecho, cada (multi)conjunto de calificaciones es una aplicación de S en $\{0, 1, \ldots, k\} = \{0, 1, 2, 3\}$ que a cada elemento de S le asocia el número de veces que aparece repetido (entre 0 y 3) en el multiconjunto, sujeta a la condición de que tales números sumen 3, en otras palabras, es una combinación con repetición y como $|S| = 3$ y $3 = |S| = n \geq k = 3$, el número de (multi)conjuntos de calificaciones es el número de combinaciones con repetición, esto es, $CR(n, k) = CR(3, 3) = C(3 + 3 - 1, 3) = 5!/(3!2!) = 10$.[39]

Razonemos ahora por reducción al absurdo. Afirmamos que hay 5 computadores con el mismo (multi)conjunto de calificaciones. Supongamos que no e intentemos deducir una contradicción. En efecto, si no hay 5 computadores con el mismo (multi)conjunto de calificaciones, es que el número de computadores que ha superado las tres pruebas ha sido como mucho de $4 \cdot 10 = 40$. Y esto contradice que las han superado 46. Por tanto, por reducción al absurdo, se deduce que, en efecto, hay al menos 5 computadores con el mismo (multi)conjunto de calificaciones.

Solución.— Al menos cinco de los 46 computadores que superaron las pruebas, lo hicieron con el mismo (multi)conjunto de calificaciones. ■

Observación 19.8.2.— Pudiésemos utilizar el artefacto en línea SageMath[40] y el siguiente programita en lenguaje Sage, para obtener estas 10 soluciones.

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
Combinations(['A','A','A','B','B','B','C','C','C'], 3).list()
```

---

[39] Alternativamente, por ejemplo, según la modelización II, el (multi)conjunto de calificaciones $\{\{A, A, B\}\}$ es una distribución simple de $k = 3$ objetos indistinguibles (por ejemplo, de un multiconjunto de tres unos, $O = \{\{1, 1, 1\}\}$, correspondiendo a las tres pruebas) en $n = 3$ recipientes distinguibles (el conjunto de las calificaciones, $R = \{A, B, C\}$), de forma que en el «recipiente» A habría 2 unos, en el B un uno y en el C, cero unos. Como, además, la aplicación subyacente $f : O \longrightarrow R$ no está sujeta a ninguna restricción de inyectividad (un computador puede obtener la misma calificación en dos pruebas distintas) o sobreyectividad (un computador puede no obtener una de las calificaciones en ninguna de las pruebas), entonces, el número de distribuciones simples viene dado por $CR(n, k) = CR(3, 3)$ (*cfr. supra* cuadro nº 2.a —teorema 19.47 (pág. 1198 de esta edición)—).

[40] *Cfr. supra* § 11 (pág. cii de esta edición).

Observación 19.8.3.— En vez de reducción al absurdo pudiésemos haber utilizado el principio generalizado de los cajones de Dirichlet, modelizando la situación como una distribución de $k = 46$ objetos (los computadores que han superado las pruebas) en $n = 10$ cajones (los [multi]conjuntos de calificaciones), satisfaciéndose la hipótesis del principio, a saber, $10 = n < k = 46$, por lo que según este principio, hay al menos un cajón —un (multi)conjunto de calificaciones— que contiene como mínimo $\lceil k/n \rceil = \lceil 46/10 \rceil = 5$ objetos (computadores).

Ejemplo 722

Sea $k \in \mathbb{Z}^+$. Pensemos en k objetos distinguibles en una disposición ordenada determinada $D_k = (o_1, o_2, \ldots, o_k)$. ¿Cuántas permutaciones de estos k objetos no contienen pares de objetos que fuesen consecutivos en D_k? (Por ejemplo, si $k = 4$, $D_4 = (o_1, o_2, o_3, o_4)$, y entonces, (o_2, o_4, o_1, o_3) sería una permutación con tal propiedad). Observemos que dado $i \in \{1, 2, \ldots, k-1\}$, (o_i, o_{i+1}) y (o_{i+1}, o_i) son pares distintos de objetos consecutivos en D_k.

[EFE 14.7.2020:3b (p.h.e.c.)].

Resolución.— Supongamos que la disposición ordenada original D_k corresponde a una ordenación creciente (biyectiva a la de las etiquetas numéricas de los objetos, de 1 a k).

Comencemos contando el número de permutaciones de D_k que contienen al menos p pares de objetos consecutivos en orden creciente, suponiendo que estos p pares forman d subdisposiciones $x_1, x_2, \ldots, x_d$, cada una de dos o más objetos ($\forall i \in \{0, 1, 2, \ldots, d\}, x_i \geq 2$).

Además, debemos contar no sólo los objetos en las subdisposiciones $x_1, x_2, \ldots, x_p$ que contienen los pares consecutivos, sino también cuántos objetos hay en los huecos entre las mismas, además de al principio y al final,

$$\square + x_1 + \square + x_2 + \square + \cdots + \square + x_d + \square = k;$$

esto es, notando por z_i al número de objetos en el hueco i, nos interesa el número de soluciones enteras de la ecuación

$$z_0 + x_1 + z_1 + x_2 + z_2 + \cdots + z_{d-1} + x_d + z_d = k,$$

donde, por un lado,

$$\begin{cases} x_1 + x_2 + \cdots + x_d = p + d, \\ x_i \geq 2 \quad (\forall i \in \{0, 1, 2, \ldots, d\}), \end{cases} \tag{19.12}$$

y por otro,

$$\begin{cases} z_1 + z_2 + \cdots + z_d = k - (p + d), \\ z_i \geq 0 \quad (\forall i \in \{0, 1, 2, \ldots, d\}). \end{cases} \tag{19.13}$$

Sabemos por el teorema 19.43 (pág. 1186 de esta edición) que el número de soluciones enteras de $x_1 + x_2 + \cdots + x_n = h$, siendo $\forall i \in \{1, 2, \ldots, n\}, x_i \geq m \geq 0$, con $m \cdot n \leq h$, es $CR(n, h - m \cdot n)$. Entonces:

I. el número de soluciones enteras de (19.12) —ya que $n = d$, $h = p + d$, $m = 2$ y se satisface que $2d \leq p + d$ ($d \leq p$, pues por construcción hay como mínimo un par de objetos consecutivos en cada subdisposición)— es

$$\begin{aligned} CR(d, p + d - 2d) &= C(d + p + d - 2d - 1, p + d - 2d) \\ &= C(d + p + d - 2d - 1, d - 1) \\ &= \binom{p-1}{d-1}; \end{aligned}$$

II. y el número de soluciones enteras de (19.13) —ya que $n = d + 1$, $h = k - (p + d)$, $m = 0$ y siempre que se satisfaga que $0 \cdot (d + 1) \leq k - (p + d)$, esto es, que $p + d \leq k$— es

$$\begin{aligned} CR(d + 1, k - (p + d)) &= C(d + 1 + k - (p + d) - 1, k - (p + d)) \\ &= C(d + 1 + k - (p + d) - 1, d + 1 - 1) \\ &= \binom{k-p}{d} \end{aligned}$$

(si $p + d \nleq k$, entonces el número de soluciones es 0).

Observemos que dado un número d de subdisposiciones $x_1, x_2, \ldots, x_d$, entonces, para cada forma de crearlas, se tienen $C(k - p, d)$ maneras de disponer objetos en los huecos entre ellas y al principio y al final, así que, por el principio de la multiplicación [¡esto requiere justificación! ✍], se tiene un total de $C(p - 1, d - 1) \cdot C(k - p, d)$. Pero esto, para un número dado d y orden creciente.

Por un lado, como el enunciado dice que dado $i \in \{1, 2, \ldots, k-1\}$, (o_i, o_{i+1}) y (o_{i+1}, o_i) son pares distintos de objetos consecutivos en D_k, da a entender que se consideran dos ordenaciones posibles, creciente ($\nearrow$) y decreciente ($\searrow$), entonces, cualquier posible ordenación de las d subdisposiciones es una aplicación de $\{1, 2, \ldots, d\}$ en el conjunto $\{\nearrow, \searrow\}$, esto es, una variación con repetición, siendo el número de ellas, 2^d (*cfr. supra* teorema 19.32 [pág. 1156 de esta edición]). Por otro, debemos considerar las permutaciones de las d subdisposiciones y de los $k - (p + d)$ objetos en los huecos, un total de $d + k - (p + d) = k - p$ elementos y por tanto $(k - p)!$ permutaciones.

Aplicando reiteradamente el principio de la multiplicación, se sigue que [¡esto requiere justificación! ✍] dado un número d de subdisposiciones, el número de permutaciones de la disposición original D_k que contienen al menos p objetos consecutivos es

$$\binom{p-1}{d-1} \cdot \binom{k-p}{d} \cdot 2^d \cdot (k - p)!$$

Resta considerar todos los posibles valores de d, desde una subdisposición hasta p o $k-p$ subdisposiciones, según qué valor sea menor, esto es, por el principio de la adición [¡esto requiere justificación! ✍],

$$\sum_{d=1}^{\text{mín}(p,k-p)} \binom{p-1}{d-1} \cdot \binom{k-p}{d} \cdot 2^d \cdot (k-p)!,$$

y éste sí es ya el número de permutaciones de la disposición original D_k que contienen al menos p objetos consecutivos.

Por el principio del complementario, lo que buscamos, el número de permutaciones de la disposición original D_k que no contienen pares de objetos que fuesen consecutivos en D_k, es igual al número total de permutaciones de la disposición original D_k —esto es, $k!$— menos el número de permutaciones de la disposición original D_k que contienen algún par de objetos que fuesen consecutivos en D_k.

El suceso contener algún par de objetos que fuesen consecutivos en D_k (abreviadamente, «contener algún par») es la unión de los sucesos «contener al menos un par», «contener al menos dos pares», ..., «contener al menos $k-1$ pares». Por el principio de inclusión-exclusión, el cardinal de esta unión es

$$\sum_{p=1}^{k-1}(-1)^{p+1} \sum_{d=1}^{\text{mín}(p,k-p)} \binom{p-1}{d-1} \cdot \binom{k-p}{d} \cdot 2^d \cdot (k-p)!$$

Finalmente, por el principio del complementario, como $k!$ es el número total de permutaciones de los objetos de D_k,

$$k! - \sum_{p=1}^{k-1}(-1)^{p+1} \sum_{d=1}^{\text{mín}(p,k-p)} \binom{p-1}{d-1} \cdot \binom{k-p}{d} \cdot 2^d \cdot (k-p)!$$

Solución.— $k! - \sum_{p=1}^{k-1}(-1)^{p+1} \sum_{d=1}^{\text{mín}(p,k-p)} \binom{p-1}{d-1} \cdot \binom{k-p}{d} \cdot 2^d \cdot (k-p)!$ permutaciones. ■

Actividad 19.39

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición y el principio de la multiplicación, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Observación 19.8.4.— Se trata de la sucesión A002464 catalogada en la OEIS[41]; allí podemos encontrar, por ejemplo, ya con nuestra notación, este programa de Vaclav KOTESOVEC en Mathematica[42]:

```
Table[
k!+Sum[(-1)^p*(k-p)!*Sum[2^d*Binomial[p-1,d-1]*Binomial[k-p,d],{d,1,p}],{p,1,k-1}],
{k,1,15}]
```

programa que proporciona como resultado

$$\{1, 0, 0, 2, 14, 90, 646, 5\,242, 47\,622, 479\,306, 5\,296\,790, 63\,779\,034, 831\,283\,558, 11\,661\,506\,218, 175\,203\,184\,374\}.$$

§ 19.9 Impromptu probabilístico

Ejemplo 723

Una moneda, un premio y dos personas; si sospechamos que la moneda está cargada, pedir que elijan cara o cruz y tirar la moneda y dar el premio a la persona que acertase, sería injusto; entonces, si el único instrumento para decidir a quién dar el premio es la moneda, ¿cómo debemos proceder para que sea justo?

[Cubit 131].

Resolución.— Sean p la probabilidad de salir cara y $1-p$ la de salir cruz. Si lanzamos dos veces la moneda, la probabilidad de salir $\langle$cara,cruz$\rangle$ es $p(1-p)$, igual a $(1-p)p$, esto es, la de salir $\langle$cruz,cara$\rangle$. Así, si lanzamos la moneda dos veces y una persona apuesta porque salga $\langle$cara,cruz$\rangle$ y la otra porque salga $\langle$cruz,cara$\rangle$, el juego es justo. ∎

Ejemplo 724

Dos papeles sobre una mesa, cada uno con un número entero escrito en la parte oculta, números que son distintos. Podemos dar la vuelta a un papel y ver el número, tras lo que podemos quedarnos con ese papel o elegir el otro, sabiendo que ganaremos este juego si elegimos el papel con el número mayor. ¿Es $1/2$ la probabilidad de ganar?

Resolución.— Thomas M. COVER (Pick the Largest Number, en *Open Problems in Communication and Computation*, Springer-Verlag, 1987) demostró que si antes de jugar pensamos en un número en-

[41] *Vid*. https://oeis.org/A002464.
[42] Programa cuya ejecución pudiésemos realizar en, por ejemplo, Wolfram Cloud (https://www.open.wolframcloud.com/).

tero n arbitrario y nos quedamos con el papel del que hemos mirado el número si este es mayor que n, entonces nuestra probabilidad de ganar es mayor que $1/2$.

En efecto, sean a y b los números escritos y, sin pérdida de generalidad, supongamos que $a < b$.

Puede suceder que:

0.°, $n < a$ (y, por tanto, $n < b$), en cuyo caso nos quedamos con el papel del que hemos mirado el número y la probabilidad de ganar es $1/2$;

1.°, $b < n$ (y, por tanto, $a < n$), en cuyo caso elegimos el otro papel y la probabilidad de ganar es $1/2$;

2.°, $a \leq n \leq b$, en cuyo caso, si el número escrito es mayor que n, nos quedamos con el papel del que hemos mirado el número, pero si el número escrito es menor o igual que n, elegimos el otro papel, por lo que siempre ganamos.

Si suponemos que estas tres situaciones se producen con probabilidades respectivas, digamos, p, q y r (con $p + q + r = 1$), entonces la probabilidad de ganar es $p/2 + q/2 + r$.

Como hemos elegido un n arbitrario (hemos hecho una elección al azar), la probabilidad de que n esté en $[a, b]$ (2.ª situación) no puede ser cero (esto es, necesariamente, $r > 0$).

Entonces, la probabilidad de ganar es:

$$\begin{aligned} p/2 + q/2 + r &= (p + q)/2 + r \\ &= (1 - r)/2 + r \\ &= (1 + r)/2 \\ &> 1/2 \quad [\text{por ser } r > 0]. \end{aligned}$$

Pudiésemos conocer más de este análisis y de varias variantes de la cuestión en este artículo de Pradeep MUTALIK en *Quanta Magazine* (en inglés): https://www.quantamagazine.org/solution-information-from-randomness-20150722/. ■

Ejemplo 725

Tres sobres, cada uno conteniendo un papel. Sabemos que uno de estos papeles tiene escrito un cero en sus dos caras; otro, un uno, también en ambas caras, y el tercero, un cero en una cara y un uno en la otra. Elegimos al azar un sobre, cogemos el papel que contiene y sin ver su cara oculta lo ponemos sobre una mesa. Imaginemos que es un cero lo que vemos, ¿es $1/2$ la probabilidad de que en su cara oculta esté escrito también un cero?

Resolución.— ¿Será que sí? Al ver un cero, el papel es el 00 o el 01, igualmente probables, probabilidad $\frac{1}{2}$, parece dictarnos nuestra intuición.

¿O será que no? Hay tres ceros en los sobres, dos en el papel 00 y uno en el papel 01; que el aparecido sea uno de los ceros del papel 00 es dos veces más probable que sea el único cero del papel 01; por lo tanto, la probabilidad de que el papel de la mesa sea el 00 es $\frac{2}{3}$. Resulta que ésta es la solución. ■

Observación 19.9.0.— Parece ser que este último ejemplo fue propuesto por primera vez por Joseph Louis François BERTRAND en 1889.[43] Es lo que se conoce como una *paradoja verídica*, aquélla cuya solución es contraria a la intuición. Como aparece en dicho artículo en Wikipedia, otras paradojas verídicas en probabilidad son: el problema de Monty Hall[44]; el problema de los tres prisioneros[45]; el problema de los dos niños (chico o chica)[46]; el problema de los dos sobres[47]; el problema de la bella durmiente[48].

§ 19.10 Bibliografía

- Debo mucho a la exposición de María del Carmen BATANERO BERNABÉU, Juan DÍAZ GODINO y Virginia NAVARRO-PELAYO en su libro *Razonamiento combinatorio*, por lo que éste es el primero que destaco:

[220]María del Carmen BATANERO BERNABÉU, Virginia NAVARRO-PELAYO y Juan DÍAZ GODINO. *Razonamiento combinatorio*. Síntesis, Madrid, Comunidad de Madrid (ES-M), España, 1994.

- La categorización en las cuatro modelizaciones que recoge el anterior proviene del artículo de Jean-Guy DUBOIS:

[216] Jean-Guy DUBOIS. Une systématique des configurations combinatoires simples. *Educational Studies in Mathematics*, 15:37–57, 1984. DOI:10.1007/BF00380438.

- Otras obras adecuadas para una aproximación inicial, para saber más, para una profundización «más allá» y para la práctica son:

[124] Jiří MATOUŠEK y Jaroslav NEŠETŘIL. *Invitación a la matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2008.

[151] Kenneth Howard ROSEN. *Matemática discreta y sus aplicaciones*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 5.ª ed., 2004. (La 5.ª edición es la última en español).

[43] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Bertrand's_box_paradox
[44] *VidV. v. gr.* https://en.wikipedia.org/wiki/Monty_Hall_problem.
[45] *Vid. v. gr.* https://en.wikipedia.org/wiki/Three_prisoners_problem.
[46] *Vid. v. gr.* https://en.wikipedia.org/wiki/Boy_or_girl_paradox.
[47] *Vid. v. gr.* https://en.wikipedia.org/wiki/Two_envelopes_problem.
[48] *Vid. v. gr.* https://en.wikipedia.org/wiki/Sleeping_Beauty_problem.

[155] Ralph Peter GRIMALDI. *Matemáticas discreta y combinatoria*. Addison-Wesley Iberoamericana, Wilmington, New Castle, Delaware (US-DE), Estados Unidos de América, 3.ª ed., 1997.

[156] Juan Carlos FERRANDO PÉREZ y Valentín GREGORI GREGORI. *Matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2.ª ed., 2012.

[157] Kenneth Allen ROSS y Charles Richard Bowers WRIGHT. *Matemáticas discretas*. Prentice-Hall Hispanoamericana, Naucalpan de Juárez, Estado Libre y Soberano de México (MX-MEX), Estados Unidos Mexicanos, 2.ª ed., 1990.

[158] Richard JOHNSONBAUGH. *Discrete Mathematics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 8.ª ed., 2018.

[190] James BRADLEY. *Introduction to discrete mathematics*. Addison-Wesley, Reading, Middlesex, Mancomunidad de Massachusetts (US-MA), Estados Unidos de América, 1988.

[214] José Ramón FRANCO BRAÑAS, María Candelaria ESPINEL FEBLES y Pedro Ramón ALMEIDA BENÍTEZ. *Manual de combinatoria*. Dirección General de Universidades e Investigación del Gobierno de Canarias, La Laguna - Tenerife, Canarias (ES-CN), España, 2005.

[217] Richard Anthony BRUALDI. *Introductory Combinatorics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 5.ª ed., 2010.

[218] Peter Jephson CAMERON. *Notes on combinatorics*. Autopublicación, 2013.

[219] Kenneth Paul BOGART. *Combinatorics throuhg guided discovery*. Autopublicación, 2004.

- Particularmente, sobre grafos:

  - UNIVERSIDAD POLITÉCNICA DE VALENCIA. *Aplicaciones de la teoría de grafos a la vida real - 1*, https://www.youtube.com/playlist?list=PL6kQim6ljTJu44dsVeZifHHiuDC1MEZ7q.
  - UNIVERSIDAD POLITÉCNICA DE VALENCIA. *Aplicaciones de la teoría de grafos a la vida real - 2*, https://www.youtube.com/playlist?list=PL6kQim6ljTJs2p7W1xMPhelLR-xPuhtJj.

- Las siguientes están dedicadas esencialmente a la práctica:

[150] Félix GARCÍA MERAYO, Gregorio HERNÁNDEZ PEÑALVER y Antonio NEVOT LUNA. *Problemas resueltos de matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 2018.

[154] Carlos GARCÍA GÓMEZ, Josep María LÓPEZ BESORA y Dolors PUIGJANER RIBA. *Matemática discreta*. Pearson Educación, Madrid, Comunidad de Madrid (ES-M), España, 2002.

[213] Felicidad AGUADO MARTÍN, Felipe GAGO COUSO, Manuel LADRA GONZÁLEZ, Gilberto PÉREZ VEGA, Concepción VIDAL MARTÍN y Ana María VIEITES RODRÍGUEZ. *Problemas resueltos*

de Combinatoria. Laboratorio con SageMath. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2018.

Parte IV

Ecuaciones en diferencias

De la infinidad de estrategias combinatorias, estudiamos las ecuaciones en diferencias. Son de utilidad, por ejemplo, en el estudio de la dinámica de poblaciones y en el de la difusión de epidemias. En computación, su conocimiento es de ayuda, por una parte, en el propio diseño de algoritmos y, por otra, en concreto, en el análisis de la complejidad de los algoritmos recursivos.

Capítulo 20

Modelización combinatoria: ecuaciones en diferencias

En la formulación de la ley de causalidad «Si conocemos el presente precisamente es posible predecir el futuro», lo que es falso no es la conclusión, sino la premisa. No es posible conocer el presente con todo detalle, ni siquiera en principio.

(Werner Karl Heisenberg).

El supuesto sigue siendo que es aceptable considerar conocida la ley que rige el fenómeno en estudio.

En el capítulo dedicado a razonamiento combinatorio hemos estudiado cómo solucionar algunos problemas combinatorios simples de recuento mediante dos tipos fundamentales de procedimientos combinatorios:

- los principios fundamentales (adición, complementario, multiplicación, división, restringido y generalizado de DIRICHLET) y
- los cuatro modelos estudiados (selección, distribución, partición de un (multi)conjunto, descomposición de un entero positivo).

Para cuestiones más complejas, existen otros procedimientos combinatorios, algunos de los cuales han dado origen a ramas completas de la matemática.

A modo de ejemplo, algunos de estos otros procedimientos combinatorios son:

- Procedimientos lógicos, como
  - el principio de inclusión-exclusión (DE MOIVRE, DA SILVA, SYLVESTER; de aplicación, por ejemplo, en teoría de números y teoría de probabilidades) y
  - el teorema de RAMSEY (de aplicación, por ejemplo, en problemas de particiones y teoría de grafos);
- Ecuaciones en diferencias (FIBONACCI, KEPLER, LAMÉ, LUCAS; de aplicación, por ejemplo, en probabilidad, teoría de renovación, teoría de juegos, teoría de números, particiones de conjuntos, complejidad algorítmica, economía, dinámica de poblaciones);
- Funciones generatrices (LAPLACE, DE MOIVRE, EULER; de aplicación, por ejemplo, en combinatoria, probabilidad, estadística, electrónica, cálculo de diferencias finitas, teorías físicas discretas);
- Grafos (EULER, puentes de Könisberg; con muchísimas aplicaciones);
- Árboles (KIRCHHOFF, circuitos eléctricos; CAYLEY, enumeración de los isómeros de hidrocarburos saturados);
- Procedimientos matriciales, como:
  - matrices de incidencia (de aplicación, por ejemplo, en general, en teoría de grafos, y en particular, en el estudio de circuitos eléctricos —KIRCHHOFF— o en topología —POINCARÉ—);
  - matrices estocásticas (por ejemplo, cadenas de MARKOV, estudiadas también por FRÉCHET y KOLMOGOROV y de aplicación, por ejemplo, en teoría de juegos, de linguística, paseos aleatorios, procesos de ramificación, difusión de epidemias, genética de poblaciones, cinética de gases);
  - rectángulos y cuadrados latinos (EULER);

- permanente de una matriz (de aplicación, por ejemplo, en la resolución del problema de LUCAS y de problemas de permutaciones con posiciones prohibidas).

- Procedimientos probabilísticos (de aplicación, por ejemplo, en problemas de planificación de experimentos).

De estos «otros» procedimientos combinatorios hemos trabajado ya con el principio de inclusión-exclusión.

En este capítulo trabajaremos con otro más, las ecuaciones en diferencias.

§ 20.0 Ecuación diferencial y en diferencias

Debemos tener clara la distinción entre ecuaciones diferenciales y ecuaciones en diferencias.

Para el estudio de problemas dinámicos en tiempo continuo, esto es, cuando es imprescindible en la modelización considerar la evolución de una magnitud en intervalos de tiempo infinitesimales, se usan las *ecuaciones diferenciales*. Son de aplicación, por ejemplo, en mecánica, circuitos eléctricos, flujos de calor, modelos de población, etc.

Para el estudio de problemas dinámicos en tiempo discreto, esto es, en una serie de instantes de tiempo: ..., milisegundos, segundos, minutos, horas, días, semanas, quincenas, meses, años, ..., se usan las *ecuaciones en diferencias* (finitas). Son de aplicación, por ejemplo, en probabilidad, teoría de renovación, teoría de juegos, teoría de números, particiones de conjuntos, complejidad algorítmica, economía, dinámica de poblaciones, etc.

§ 20.1 Generalidades

§ 20.1.0 Sumas de progresiones aritméticas, geométricas y aritmético-geométricas

Definición 20.0.— Una *sucesión de elementos de un conjunto* S es una aplicación $s : \mathbb{N} \longrightarrow S$, esto es, por extensión, $\{s_0, s_1, s_2, \ldots\}$ —conjunto éste que es una abreviatura del grafo de la aplicación, es decir, del conjunto de pares ordenados $\{(0, s_0), (1, s_1), (2, s_2), \ldots\}$—, o simplemente $\{s_n\}$, sobreentendiendo que $n \in \mathbb{N}$.

Observación 20.1.0.— Sabemos que la sucesión $\{s_0, s_1, s_2, \ldots\}$ no es más que la tupla infinita $\langle s_0, s_1, \ldots, s_n, \ldots\rangle_{n\in\mathbb{N}}$, que abreviadamente pudiésemos notar $\langle s_n\rangle_{n\in\mathbb{N}}$ o, alternativamente, $\{s_n\}_{n\in\mathbb{N}}$ o simplemente $\{s_n\}$.

Definición 20.1.— Llamamos suma parcial de una sucesión a una suma de términos.

Definición 20.2.— Dada una sucesión $\{a_n\}$, siempre es posible construir una nueva sucesión $\{b_n\}$ así

$$b_n = a_0 + a_1 + a_2 + \cdots + a_n.$$

El término b_n se llama *suma parcial enésima* de a_n. Como los términos de $\{b_n\}$ son las sumas de la parte inicial de la sucesión $\{a_n\}$, se llama a $\{b_n\}$ la *sucesión de sumas parciales de* $\{a_n\}$.

Definición 20.3.— Una sucesión $\{s_n\}$ es una *progresión aritmética* precisamente si la diferencia entre los términos consecutivos es constante. Esto se traduce inmediatamente en su definición recursiva $s_0 = a$, $s_n = s_{n-1} + d$ $(n \geq 1)$, con $a, d \in \mathbb{R}$, siendo su término general $s_n = a + nd$.

Teorema 20.0

Dada $s_n = a + nd$, la suma parcial de los n primeros términos de $\{s_n\}$, $S_n = a_0 + a_1 + a_2 + \cdots + a_{n-1} = a + (a+d) + (a+2d) + \cdots + (a+(n-1)d)$, tiene como fórmula $S_n = n(a_0 + a_{n-1})/2$, esto es,

$$S_n = \frac{n(2a + (n-1)d)}{2}.$$

Observación 20.1.1.— Un par de casos particulares del teorema son:

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},$$
$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

Definición 20.4.— Una sucesión $\{s_n\}$ es una *progresión geométrica* precisamente si la razón entre los términos sucesivos es constante. Esto se traduce inmediatamente en su definición recursiva $s_0 = b$, $s_n = rs_{n-1}$ $(n \geq 1)$, con $b, d \in \mathbb{R}$, siendo su término general $s_n = br^n$.

Teorema 20.1

Dada $s_n = br^n$, con $r \neq 1$, la suma parcial de los n primeros términos de $\{s_n\}$, $S_n = b_0 + b_1 + b_2 + \cdots + b_{n-1} = b + br + br^2 + \cdots + br^{n-1}$, tiene como fórmula $S_n = (b_0 - r \cdot b_{n-1})/(1-r)$, esto es,

$$S_n = \frac{b(1 - r^n)}{1 - r}.$$

Observación 20.1.2.— Si $-1 < r < 1$, la serie geométrica, $\sum br^n$, converge y su suma es $S = \dfrac{b}{1-r}$.

Observación 20.1.3.— Si consultamos otros textos, pudiese ser que encontrásemos otras fórmulas para estas progresiones; en concreto, pudiésemos encontrar, como términos generales, $a_n = a + (n-1)d$ para la progresión aritmética y $b_n = b \cdot r^{n-1}$ para la geométrica. Aunque diferentes,

todas estas fórmulas son correctas: las nuestras, comenzando en $n = 0$ y las suyas, comenzando en $n = 1$.

Definición 20.5.— Una sucesión $\{s_n\}$ es una *progresión aritmético-geométrica* precisamente si existen dos sucesiones, $\{a_n\}$ y $\{b_n\}$, aquélla una progresión aritmética y ésta una progresión geométrica, tales que $s_n = a_n b_n$.

Si $a_n = a + dn$ y $b_n = br^n$, entonces el *término general* de $\{s_n\}$ es $s_n = (a+dn)br^n$. Observemos que $a_0 = a$, $b_0 = b$ y $s_0 = a_0 b_0$ y que $r \neq 1$ (si fuese 1 sería una progresión aritmética).

Teorema 20.2
Dada $s_n = (a + dn)br^n$, con $r \neq 1$, la suma parcial de los n primeros términos de $\{s_n\}$, $S_n = s_0 + s_1 + s_2 + \cdots + s_{n-1} = ab + (a+d)br + (a+2d)br^2 + \cdots + (a+(n-1)d)br^{n-1}$, tiene como fórmula

$$S_n = \frac{ab(1-r^n)}{1-r} + \frac{dbr(1 - nr^{n-1} + (n-1)r^n)}{(1-r)^2}.$$

Observación 20.1.4.— Si $-1 < r < 1$, la serie aritmético-geométrica, $\sum (a+dn)br^n$, es convergente y su suma es $S = \dfrac{ab}{1-r} + \dfrac{bdr}{(1-r)^2}$.

§ 20.1.1 Sumas de potencias

Otras sumas interesantes son las de potencias.

Definición 20.6.— Los *números de* BERNOULLI[○] se definen por

$$\binom{2n+1}{2} 2^2 B_1 - \binom{2n+1}{4} 2^4 B_2 + \binom{2n+1}{6} 2^6 B_3 - \cdots + (-1)^{n-1}(2n+1)2^{2n} B_n = 2n.$$

A modo de ejemplo, los siete primeros números de Bernoulli son: $B_1 = 1/6$, $B_2 = 1/30$, $B_3 = 1/42$, $B_4 = 1/30$, $B_5 = 5/66$, $B_6 = 691/2730$ y $B_7 = 7/6$.

Teorema 20.3
$\forall k \in \mathbb{Z}^+$ se satisface

$$1^k + 2^k + 3^k + \cdots + n^k = \frac{n^{k+1}}{k+1} + \frac{1}{2}n^k + \frac{B_1 k n^{k-1}}{2!} - \frac{B_2 k(k-1)(k-2)n^{k-3}}{4!} + \cdots,$$

donde B_i son los números de Bernoulli.

[○] Con ánimo de simplificar las expresiones, notamos B_n lo que en muchos lugares se nota B_{2n} (por ejemplo, en https://en.wikipedia.org/wiki/Bernoulli_number).

Observación 20.1.5.— Algunos casos particulares son:

$$\begin{aligned} 1+2+3+\cdots+n &= \frac{n(n+1)}{2}, \\ 1^2+2^2+3^2+\cdots+n^2 &= \frac{n(n+1)(2n+1)}{6}, \\ 1^3+2^3+3^3+\cdots+n^3 &= \frac{n^2(n+1)^2}{4}, \\ 1^4+2^4+3^4+\cdots+n^4 &= \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}. \end{aligned}$$

Observación 20.1.6.— Por cierto, otras sumas de potencias de interés que se satisfacen son:

$$\begin{aligned} 1+3+5+7+\cdots+(2n-3)+(2n-1) &= n^2, \\ 2+4+6+8+\cdots+(2n-2)+2n &= n(n+1), \\ 1^3+2^3+3^3+\cdots+n^3 &= (1+2+3+\cdots+n)^2, \\ 1^2+3^2+5^2+7^2+\cdots+(2n-3)^2+(2n-1)^2 &= \frac{n(4n^2-1)}{3}, \\ 1^3+3^3+5^3+7^3+\cdots+(2n-3)^3+(2n-1)^3 &= n^2(2n^2-1). \end{aligned}$$

§ 20.1.2 Ecuaciones cuadráticas y cúbicas

Dado que aparecerá la resolución de ciertas ecuaciones, recordemos las fórmulas de CARDANO-VIETA para la ecuación cuadrática $a_2x^2+a_1x+a_0=0$, siendo r_0 y r_1 las soluciones reales:

$$\begin{aligned} r_0+r_1 &= -\frac{a_1}{a_2}, \\ r_0\cdot r_1 &= \frac{a_0}{a_2}, \end{aligned}$$

y para la ecuación cúbica $a_3x^3+a_2x^2+a_1x+a_0=0$, siendo r_0, r_1 y r_2 las soluciones reales:

$$\begin{aligned} r_0+r_1+r_2 &= -\frac{a_2}{a_3}, \\ r_0\cdot r_1+r_0\cdot r_2+r_1\cdot r_2 &= \frac{a_1}{a_3}, \\ r_0\cdot r_1\cdot r_2 &= -\frac{a_0}{a_3}. \end{aligned}$$

Si nos suscitan interés, pudiésemos aprender más sobre estas fórmulas[1]. También más sobre las ecuaciones cuadrática[2] y cúbica[3]. Tampoco nos olvidemos de la *regla de* RUFFINI[4] y de otras estrategias de factorización[5].

[1] *Vid. v. gr.* https://es.wikipedia.org/wiki/Relaciones_de_Cardano-Vieta.
[2] *Vid. v. gr.* https://es.wikipedia.org/wiki/Ecuación_de_segundo_grado.
[3] *Vid. v. gr.* https://es.wikipedia.org/wiki/Ecuación_de_tercer_grado.
[4] *Vid. v. gr.* https://es.wikipedia.org/wiki/Regla_de_Ruffini.
[5] *Vid. v. gr.* https://es.wikipedia.org/wiki/Factorización.

§ 20.2 Ecuación en diferencias (ED)

Definición 20.7.— Dada una función $h : \mathbb{N} \longrightarrow \mathbb{R}$, llamamos *ecuación en diferencias* (o, sinónimamente, *ecuación recurrente*, *ecuación de recurrencia*, *relación recurrente* o *relación de recurrencia*), a toda expresión que relacione un término cualquiera a_n con n y con uno o más términos anteriores,

$$G(n, h(n-k), \ldots, h(n-2), h(n-1), h(n)) = 0,$$

o con uno o más términos posteriores,

$$G(n, h(n), h(n+1), h(n+2), \ldots, h(n+k)) = 0,$$

donde G permite expresiones complejas como, por ejemplo, $h(n) = n - h(h(h(n-1)))$ o $h(n) = h(n - h(n-1)) + h(n - h(n-2))$.

El nombre proviene de que son expresables en función del *operador diferencia* «progresiva» $\triangle h(n) = h(n+1) - h(n)$.

Definición 20.8.— Llamamos *orden* de una ecuación en diferencias a la diferencia $|k - k'|$ correspondiente a los términos de índices mayor y menor.

§ 20.2.0 Linealidad (L)

Definición 20.9.— Decimos que una ecuación en diferencias es una *ecuación en diferencias lineal* (EDL) cuando puede escribirse en la forma

$$c_0(n)h(n) + c_1(n)h(n-1) + c_2(n)h(n-2) + \cdots + c_k(n)h(n-k) = F(n)$$

con h, $c_0, c_1, \ldots, c_k$ y F, aplicaciones conocidas de $\mathbb{N}$ en $\mathbb{R}$.

Ejemplo 726

¿Qué estructura tienen las ecuaciones $h(n) = h(n-1)h(n-2)$ y $h(n-1) = 2h(n-3) + 5n$?

Resolución.— La ecuación en diferencias $h(n) = h(n-1)h(n-2)$ no es lineal y su orden es $|0-2| = 2$; la ecuación en diferencias $h(n-1) = 2h(n-3)+5n$ es lineal y su orden es $|1-3| = 2$. ■

Observemos que siendo lineal, en la ecuación en diferencias no aparece ningún producto entre términos en ninguno de los sumandos.

Es frecuente notar $h(n)$ por h_n.

§ 20.2.1 Homogeneidad (H)

Definición 20.10.— Si en todos los sumandos aparece un término $h(n)$, esto es, si $F(n) = 0$, decimos que es una *ecuación en diferencias homogénea*; en caso contrario, decimos que es *no homogénea*, *general* o *completa*. Llamamos a $F(n)$ el *término no homogéneo* o *término independiente* de la ecuación.

Ejemplo 727

¿Qué estructura tiene la ecuación $h(n) = 2h(n-3) + 5n$?

Resolución.— Se trata de una ecuación en diferencias lineal completa de orden $|0-3| = 3$; el término no homogéneo es $5n$. ■

Definición 20.11.— Dada la ecuación en diferencias lineal no homogénea

$$c_0(n)h(n) + c_1(n)h(n-1) + c_2(n)h(n-2) + \cdots + c_k(n)h(n-k) = F(n),$$

decimos que

$$c_0(n)h(n) + c_1(n)h(n-1) + c_2(n)h(n-2) + \cdots + c_k(n)h(n-k) = 0$$

es su ecuación en diferencias *homogénea asociada* (HA). A la ecuación con la parte homogénea la llamamos *ecuación en diferencias (lineal) completa*.

§ 20.2.2 Coeficientes constantes (CC)

Definición 20.12.— Cuando todos los coeficientes $c_i(n)$ son constantes, esto es, cuando la ecuación es $c_0h(n) + c_1h(n-1) + c_2h(n-2) + \cdots + c_kh(n-k) = F(n)$, con $c_0, c_1, \ldots, c_k \in \mathbb{R}$, decimos que es una *ecuación en diferencias lineal con coeficientes constantes* (EDL-CC).

Ejemplo 728

¿Qué estructura tiene la ecuación $h(n) = h(n-1) + 2nh(n-3) + 5$?

Resolución.— Se trata de una ecuación en diferencias lineal no homogénea de orden $|0-3| = 3$ con coeficientes no constantes; el término no homogéneo es 5. ■

§ 20.2.3 Problema de valores iniciales (PVI)

Definición 20.13.— Llamamos *problema de valores iniciales* (PVI) a una ecuación en diferencias junto a un conjunto finito de *condiciones/valores iniciales* de $h(n)$: $h(0), h(1), \ldots$

Teorema 20.4 (Teorema CERO —existencia y unicidad de la solución—)
Dada la ecuación en diferencias lineal completa

$$c_0(n)h(n) + c_1(n)h(n-1) + c_2(n)h(n-2) + \cdots + c_k(n)h(n-k) = F(n),$$

de orden k —esto es, siendo $c_0(n) \neq 0$ y $c_k(n) \neq 0$—, entonces el problema de valores iniciales formado por dicha ecuación y k condiciones iniciales correspondientes a k enteros consecutivos, $h(n_0) = c_0, h(n_0+1) = c_1, \ldots, h(n_0+k-1) = c_{k-1}$, tiene solución y ésta es única.

Observación 20.2.0.— Para la existencia de solución y su unicidad, dos son las exigencias impuestas por este teorema, a saber:

0.º, el número de condiciones iniciales debe ser igual al orden, k, y

1.º, las k condiciones iniciales deben ser consecutivas.

§ 20.3 Resolución de EDL y PVI: métodos elementales

§ 20.3.0 Sustitución hacia adelante (SHA)

La estrategia de *sustitución hacia adelante* (SHA) —llamada a veces simplemente, *iteración*— se lleva a cabo en tres fases:

(E) *Expansión hacia adelante*, por ejemplo, $a_1 = \phi(a_0)$, $a_2 = \phi(a_1)$, $a_3 = \phi(a_2), \ldots$;

(I) *Intuición*, por ejemplo, $a_n = \varphi(n)$, y

(D) *Demostración* de lo intuido (habitualmente por inducción).

Veamos un ejemplo.

Ejemplo 729

El número de gusanos en una colonia localizada de programas malignos (*malware*) oculta en una red se duplica cada segundo. Suponiendo que al comienzo la colonia tuviese sólo un gusano, ¿cuántos tendría después de n segundos sin considerar limitaciones de recursos computacionales?

> «Un gusano es un tipo de programa maligno que se replica en el sistema, adjuntándose a diferentes archivos y buscando vías de comunicación entre los computadores, como una red de computadores que comparta áreas comunes de almacenamiento de archivos. Los gusanos suelen ralentizar las redes. Un virus necesita un programa anfitrión para ejecutarse, pero los gusanos pueden ejecutarse por sí mismos. Después de que un gusano afecta a un anfitrión, es capaz de propagarse muy rápidamente por la red» (https://www.geeksforgeeks.org/malware-and-its-types/).

[Cubit 150].

Resolución.— Sea $g(n)$ el n.º de gusanos en el segundo n. Notemos $g(n)$ por g_n —llegado un momento adoptaremos esta notación, habitual con sucesiones numéricas—.

Como su número se duplica cada segundo,

$$g_n = 2g_{n-1}, \tag{20.0}$$

para todo n entero positivo y sabemos que

$$g_0 = 1. \tag{20.1}$$

Estamos ante un problema de valores iniciales —*cfr. supra* definición 20.13 (pág. 1302 de esta edición)—.

Encontremos una expresión explícita, una fórmula cerrada, para g_n, por sustitución hacia adelante (SHA).

0. *Expansión hacia adelante*.

$$\begin{aligned} g_1 &= 2 \cdot g_0 = 2^1 \cdot g_0 \\ g_2 &= 2 \cdot g_1 = 2 \cdot (2^1 \cdot g_0) = 2^2 \cdot g_0 \\ g_3 &= 2 \cdot g_2 = 2 \cdot (2^2 \cdot g_0) = 2^3 \cdot g_0 \\ &\vdots \end{aligned}$$

1. *Intuición*.— Intuimos que $g_n = 2^n \cdot g_0$, y por (20.1), nuestra intuición definitiva es que para todo $n \in \mathbb{N}$,

$$g_n = 2^n. \tag{20.2}$$

2. *Demostración*.— Debemos demostrar lo intuido, que $g_n = 2^n$, para todo $n \in \mathbb{N}$, por ejemplo, por inducción débil. Veamos, como por un lado, de (20.1), $g_0 = 1$ y por otro, de (20.2), $g_0 = 2^0$, que también es 1, se sigue el paso base de la inducción. Para demostrar el paso inductivo, tomamos como hipótesis inductiva que $g_i = 2^i$ y demostramos que $g_{i+1} = 2^{i+1}$; en efecto, de (20.0), $g_{i+1} = 2g_i$, de donde, por hipótesis inductiva, $g_{i+1} = 2 \cdot 2^i$, es decir, $g_{i+1} = 2^{i+1}$. Al satisfacerse el paso base y el paso inductivo, las hipótesis de la inducción débil, concluimos por ésta lo intuido, que para todo $n \in \mathbb{N}$, $g_n = 2^n$.

Esta fase final de demostración es crucial, pues, de lo contrario, todo hubiese quedado en una intuición, una mera conjetura. ■

Observación 20.3.0.— El método de sustitución hacia adelante tiene un condicionante fuerte, a saber, la tercera fase, es necesario demostrar lo intuido, algo crucial como ya hemos comentado, pues de lo contrario, insistimos, todo quedaría en una mera intuición.

Ayes de la intuición

Sí, claro que la intuición es necesaria, en la mayoría de las ocasiones es la mejor guía, pero a veces puede, ¿fallar?

En dos dimensiones euclídeas, en $\mathbb{R}^2$, dividimos un cuadrado de lado 4 en cuatro cuadrados de lado 2 iguales; en cada uno de ellos inscribimos un círculo unitario (de radio $R = 1$); entre estos cuatro círculos inscribimos un círculo tangente a los cuatro de radio r; pudiésemos demostrar que $r = \sqrt{2} - 1$.

En efecto, la diagonal del cuadrado de vértices los centros de los cuatro círculos mide $2r + 2R$; este cuadrado tiene lado 2, por lo que su diagonal mide $2 \cdot \sqrt{2}$ (✍); por lo tanto, $2r + 2R = 2 \cdot \sqrt{2}$, esto es, $r + R = \sqrt{2}$; como $R = 1$, $r = \sqrt{2} - 1$.

En tres dimensiones euclídeas, en $\mathbb{R}^3$, dividimos un cubo de lado 4 en ocho cubos de lado 2 iguales; en cada uno de ellos inscribimos una bola unitaria (de radio $R = 1$); entre estas ocho bolas inscribimos una bolita tangente a las ocho de radio r; pudiésemos demostrar que $r = \sqrt{3} - 1$.

En efecto, la diagonal del cubo de vértices los centros de las ocho bolas mide $2r + 2R$; este cubo tiene lado 2, por lo que su diagonal mide $2 \cdot \sqrt{3}$ (✍); por lo tanto, $2r + 2R = 2 \cdot \sqrt{3}$, esto es, $r + R = \sqrt{3}$; como $R = 1$, $r = \sqrt{3} - 1$.

Y así sucesivamente.

En n dimensiones euclídeas, en $\mathbb{R}^n$, el radio de la bolita es $r = \sqrt{n} - 1$.

He aquí lo contrario a nuestra intuición:

- en 5 o más dimensiones euclídeas, esto es, si $n \geq 5$, la bolita es «más grande» que las bolas (su radio es mayor que el de ellas: $r = \sqrt{5} - 1 \approx 1{,}236068 > 1$);

- pero no sólo esto, en 10 o más dimensiones euclídeas, esto es, si $n \geq 10$, la bolita «desborda» el cubo donde están todas las bolas, «se sale» de dicho cubo ($r = \sqrt{10} - 1 \approx 2{,}162278 > 2$).

Claro que no debería sorprendernos en demasía, por ejemplo, en $\mathbb{R}^4$ ya es posible desenganchar dos anillos enganchados sin romperlos (ese truco de magia tan popular) o invertir/evertir una esfera sin romperla (esto es, darle la vuelta a la esfera sin romperla) (si bien Stephen SMALE en su tesis doctoral, 1957, demostró que esto era posible en $\mathbb{R}^3$: https://proyectodescartes.org/uudd/materiales_didacticos/superficies-curiosas-2_JS/images/la_inversion_de_la_esfera.pdf).

§ 20.3.1 Sustitución hacia atrás (SHT)

Similarmente a la sustitución hacia adelante, la estrategia de *sustitución hacia atrás* (SHT) se lleva a cabo en tres fases:

(E) *Expansión hacia atrás*, por ejemplo, $a_n = \phi(a_{n-1}) = \phi(\phi(a_{n-2})) = \phi(\phi(\phi(a_{n-3}))) = \ldots$;

(I) *Intuición*, por ejemplo, $a_n = \varphi(n)$, y

(D) *Demostración* de lo intuido (habitualmente por inducción).

Utilicemos esta estrategia con el ejemplo 729 (pág. 1303 de esta edición).

Ejemplo 730 (729 bis)

El número de gusanos en dicha colonia localizada de programas malignos oculta en una red se duplica cada segundo. Suponiendo que al comienzo la colonia tuviese sólo un gusano, ¿cuántos tendría después de n segundos sin considerar limitaciones de recursos informáticos?

[Cubit 151].

Resolución.— Sea g_n el n.º de gusanos en el segundo n; como dicho número se duplica cada segundo, $g_n = 2g_{n-1}$, para todo n entero positivo y sabemos que $g_0 = 1$.

De nuevo estamos ante un problema de valores iniciales.

Buscamos una expresión explícita para g_n por sustitución hacia atrás (SHT).

0. *Expansión hacia atrás*.

$$\begin{aligned} g_n &= 2 \cdot g_{n-1} = 2^1 \cdot g_{n-1} \\ &= 2 \cdot (2 \cdot g_{n-2}) = 2^2 \cdot g_{n-2} \end{aligned}$$

$$= 2^2 \cdot (2 \cdot g_{n-3}) = 2^3 \cdot g_{n-3}$$
$$\vdots$$

1. *Intuición*. Expandimos hasta que intuimos, en este caso que g_n es de la forma

$$g_n = 2^k \cdot g_{n-k};$$

como este descenso es finito y termina cuando $g_{n-k} = g_0$, y como si $n-k = 0$, $k = n$, entonces

$$g_n = 2^n \cdot g_0,$$

y como $g_0 = 1$, intuimos que $g_n = 2^n$, para todo $n \in \mathbb{N}$.

2. *Demostración*. Debemos demostrar lo intuido, esto es, que $g_n = 2^n$, para todo $n \in \mathbb{N}$, por ejemplo, por inducción débil —*cfr. infra* actividad 20.0 (pág. 1306 de esta edición)—. ■

Actividad 20.0

Completemos la tercera fase, demostración, del ejemplo inmediatamente anterior.

Observación 20.3.1.— La sustitución hacia atrás tiene el mismo condicionante fuerte que la sustitución hacia adelante, a saber, la tercera fase, es necesario demostrar lo intuido, algo crucial como hemos dicho, pues de lo contrario, debemos insistir, todo quedaría en una mera intuición.

§ 20.3.2 Estrategia telescópica (TEL)

La *estrategia telescópica* (TEL) se lleva a cabo en tres fases:

(E) *Expansión telescópica*, por ejemplo, $a_1 - a_0 = d_0$, $a_2 - a_1 = d_1$, $a_3 - a_2 = d_2, \ldots, a_n - a_{n-1} = \phi(n-1)$;

(Σ) *Suma*, miembro a miembro, todas las igualdades, por ejemplo, $a_n - a_0 = \varphi(n)$, y

(S) *Sustitución*, de a_0 en $a_n - a_0$, obteniendo a_n.

Ejemplifiquemos esta estrategia con una variación del ejemplo 729 (pág. 1303 de esta edición).

En vez de n, usemos t para los instantes de tiempo discreto, así $t-1$ indica la unidad de tiempo (.../segundo/minuto/hora/día/...) inmediatamente anterior a t y $t+1$ la inmediatamente posterior a t, en vez de g_n usemos N_t para notar la población de gusanos en la colonia, esto es, el número bruto de individuos —gusanos informáticos, en nuestro caso— en el instante t (N_t se conoce como la abundancia actual).

Además de N_t, consideremos ahora B_t, D_t, I_t y E_t, como el número de gusanos creados («nacidos»), desaparecidos («muertos»), nuevos en la colonia procedentes del exterior («inmigrados»),

antiguos miembros de la colonia localizados fuera en otro lugar de la red («emigrados»), en *dinámica de poblaciones*, éste se conoce como *modelo* BIDE (*Births*, *Immigration*, *Deaths*, *Emigration*),

$$N_t = N_{t-1} + B_{t-1} - D_{t-1} + I_{t-1} - E_{t-1} \qquad (t \in \mathbb{Z}^+);$$

de hecho, para no escribir tantos $t-1$, suele utilizarse la forma progresiva

$$N_{t+1} = N_t + B_t - D_t + I_t - E_t \qquad (t \in \mathbb{N}).$$

Observación 20.3.2.— La afirmación $g_0 = 1$, que se traduce en $N_0 = 1$, implica que si no sucede nada en la colonia, entonces $g_1 = 1$, ya que $N_1 = N_0 + B_0 - D_0 + I_0 - E_0 = 1 + 0 - 0 + 0 - 0 = 1$.

Observación 20.3.3.— Si el área poblacional es muy grande —en el ejemplo 729 (pág. 1303 de esta edición), si la infección está muy extendida en la red—, o en todo caso, cuando los desplazamientos poblacionales no se consideren de importancia, pudiésemos despreciar la inmigración y la emigración, y si por otro lado, trabajásemos con tasas per cápita, la ecuación quedaría $N_{t+1}/N_t = 1 + B_t/N_t - D_t/N_t$, que suele expresarse $N_{t+1}/N_t = 1 + r_t$, siendo r_t la tasa finita de incremento y, entonces, la ecuación quedaría $N_{t+1} = N_t + N_t r_t$; si las tasas de nacimiento y muerte permaneciesen constantes (no dependencia de la densidad), $B_t/N_t = b$ y $D_t/N_t = d$, entonces $r_t = b-d$ sería constante, r, y la ecuación sería $N_{t+1} = N_t(1+r)$, la cual, si el valor inicial (abundancia inicial) es N_0, tiene como solución $N_t = N_0(1+r)^t$ (lo que pudiésemos demostrar por sustitución hacia adelante).

Existen muchos más modelos: si tales tasas no son constantes (dependencia de la densidad), si considerásemos estratificaciones por edad, si incluyésemos factores no predecibles, si surgen divisiones independientes de la colonia, modelos de múltiples especies de individuos (predador-presa, competencia, alianzas/coaliciones, ...), etc.[6]

[6] Por otra parte, no nos olvidemos de la teoría evolutiva de juegos (*cfr. v. gr.* https://es.wikipedia.org/wiki/Teoría_evolutiva_de_juegos).

Ejemplo 731 (729 ter)

Supongamos que en dicha colonia localizada de programas malignos oculta en la red, hemos conseguido implantar una contramedida que «marca» los gusanos nada más que se crean o detectamos su llegada o salida de la colonia, y observamos una pauta fija, a saber, observando el instante t, el número de gusanos creados es el mismo que el de desaparecidos y sorprendentemente, el número de inmigrados es $2t$ y el de emigrados t. Seguimos suponiendo que al comienzo de la colonia había un gusano (esto es, $N_0 = 1$). La cuestión es, ¿cuántos habría después de n segundos sin tener en cuenta limitaciones de recursos informáticos?

[Cubit 152].

Resolución.— Tenemos, pues, que $N_t = B_t$, $I_t = 2t$ y $E_t = t$, para todo t, por tanto, $N_t = N_{t-1} + B_{t-1} - D_{t-1} + I_{t-1} - E_{t-1}$ queda

$$N_t = N_{t-1} + t - 1,$$

ya que $2(t-1) - (t-1) = t - 1$.

Apliquemos la estrategia telescópica.

0. *Expansión telescópica*.— Iteramos $N_t - N_{t-1} = t - 1$ recorriendo los valores de t:

$$\begin{aligned} N_1 - N_0 &= 1 - 1 = 0, \\ N_2 - N_1 &= 2 - 1 = 1, \\ N_3 - N_2 &= 3 - 1 = 2, \\ N_4 - N_3 &= 4 - 1 = 3, \\ &\vdots \\ N_t - N_{t-1} &= t - 1. \end{aligned}$$

1. *Suma*.— Sumamos todas las igualdades para, por un lado, anular muchos términos,

$$(N_1 - N_0) + (N_2 - N_1) + \cdots + (N_{t-1} - N_{t-2}) + (N_t - N_{t-1}) = N_t - N_0,$$

y por otro, obtener una suma parcial conocida de una serie,

$$0 + (1 + 2 + 3 + \cdots + t) - 1,$$

quedando que

$$N_t - N_0 = 0 + (1 + 2 + 3 + \cdots + t) - 1. \tag{20.3}$$

Observemos que $(1+2+3+\cdots+t)$ es la suma parcial tésima de una progresión aritmética de diferencia 1, y esta suma es

$$\frac{t(t+1)}{2}. \tag{20.4}$$

2. *Sustitución*.— Sustituimos (20.4) en (20.3), por lo que

$$N_t - N_0 = 0 + \frac{t(t+1)}{2} - 1,$$

y ahora incorporamos la condición inicial, esto es, en este caso, sustituimos N_0 por su valor, a saber, 1,

$$N_t - 1 = 0 + \frac{t(t+1)}{2} - 1,$$

y por tanto,

$$N_t = \frac{t(t+1)}{2}.$$

Hemos conseguido hallar una expresión explícita, una fórmula cerrada, para N_t. ■

Observación 20.3.4.— La estrategia telescópica tiene dos condicionantes fuertes, a saber, la ecuación en diferencias debe ser ajustable para que, 0.°, por un lado, la expresión en el lado izquierdo de la igualdad sea «plegable» telescópicamente y, 1.°, por otro, la suma parcial que se obtiene en el lado derecho debe ser conocida.

Observación 20.3.5.— En el ejemplo 729 (pág. 1303 de esta edición), $g_n = 2g_{n-1}$ no se pliega telescópicamente, así que no es admisible aplicar la estrategia telescópica.

Observación 20.3.6.— La sucesión $\{N_n\}$ está catalogada en la OEIS como la sucesión A152947[7].

El término $n+1$ de esta sucesión es precisamente el enésimo número poligonal central, esto es,

$$N_{n+1} = {}_cP_1^{(2)}(n),$$

donde $\{{}_cP_1^{(2)}(n)\}$ es la *sucesión de los números unigonales centrales*[8], que se definen tradicionalmente como la solución única del PVI (comparémosla con la de N_n)

$$\begin{aligned} {}_cP_1^{(2)}(n) &= {}_cP_1^{(2)}(n-1) + n \quad (n \geq 1), \\ {}_cP_1^{(2)}(0) &= 1, \end{aligned}$$

cuya expresión explícita más frecuente es

$${}_cP_1^{(2)}(n) = \frac{n(n+1)}{2} + 1,$$

[7] *Vid*. https://oeis.org/A152947.
[8] *Cfr. v. gr.* https://oeis.org/wiki/Centered_polygonal_numbers.

y que están catalogados en la OEIS como la sucesión A000124[9].

Otra interpretación de ${}_cP_1^{(2)}(n)$ es el máximo número de piezas en que puede dividirse un disco con n cortes rectos tipo guillotina[10].

[Cubit 153], [Cubit 154].

Observación 20.3.7.— Por otra parte,

$$ {}_cP_1^{(2)}(n) = T_n + 1, $$

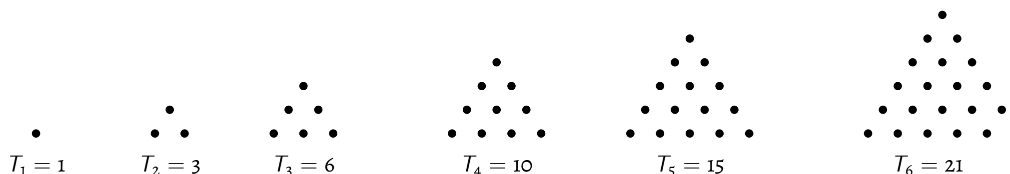
donde T_n es la *sucesión de los números triangulares*[11], que se definen tradicionalmente como la solución única del PVI (comparémosla con la de a_n y N_n)

$$ \begin{aligned} T_n &= T_{n-1} + n \quad (n \geq 1), \\ T_0 &= 0, \end{aligned} $$

cuya expresión explícita más frecuente es

$$ T_n = \frac{n(n+1)}{2}, $$

y que están catalogados como la sucesión A000217 en la OEIS[12].



Teorema 20.5 (Gauss)
Todo número natural es suma de como mucho tres números triangulares.
(Por ejemplo: $0 = 0; 1 = 1; 2 = 1 + 1; 3 = 3; 4 = 1 + 3; 5 = 1 + 1 + 3$, y así sucesivamente).

Teorema 20.6
Todo cuadrado perfecto es suma de dos números triangulares consecutivos.
(Por ejemplo: $1^2 = 0 + 1; 2^2 = 1 + 3; 3^2 = 3 + 6; 4^2 = 6 + 10; 5^2 = 10 + 15; 6^2 = 15 + 21; 7^2 = 21 + 28$, y así sucesivamente).

Enumerativamente:

---

9 *Vid*. https://oeis.org/A000124.
10 *Cfr. v. gr.* https://es.wikipedia.org/wiki/Teorema_del_cortador_perezoso.
11 *Vid. v. gr.* https://es.wikipedia.org/wiki/N%C3%BAmero_triangular.
12 *Vid*. https://oeis.org/A000217.

$n \in \mathbb{Z}^+$	$n \in \mathbb{N}$	0	1	2	3	4	5	6	7	8	9	...
$\begin{cases} T_n = T_{n-1} + n, \\ T_0 = 0. \end{cases}$	$T_n = \dfrac{n(n+1)}{2}.$	0	1	3	6	10	15	21	28	36	45	...
$\begin{cases} {}_cP_1^{(2)}(n) = {}_cP_1^{(2)}(n-1) + n, \\ {}_cP_1^{(2)}(0) = 1. \end{cases}$	${}_cP_1^{(2)}(n) = \dfrac{n(n+1)}{2} + 1.$ Obs.: ${}_cP_1^{(2)}(n) = T_n + 1.$	1	2	4	7	11	16	22	29	37	46	...
$\begin{cases} N_n = N_{n-1} + n - 1, \\ N_0 = 1. \end{cases}$	$N_n = \dfrac{n(n-1)}{2} + 1.$ Obs.: $N_{n+1} = {}_cP_1^{(2)}(n).$	1	1	2	4	7	11	16	22	29	37	...

[Cubit 155].

Observación 20.3.8.— En las diagonales del *triángulo de Pascal* aparecen, entre otros, los números enteros positivos, los números triangulares, los *números tetraédricos* (1, 4, 10, 20, 35, 56, 84, 120, 165, 220 . . .)[13] y los *números pentatópicos* (1, 5, 15, 35, 70, 126, 210, 330, 495, 715 . . .)[14]. Por otra parte, los números unigonales centrales y los números triangulares aparecen en la disposición conocida como *triángulo de Floyd*[15]. También aparecen sucesiones de interés en el *triángulo de Bernoulli*[16]. Existen más triángulos interesantes de números[17].

§ 20.4 Resolución de EDL y PVI: coeficientes indeterminados

§ 20.4.0 EDL-H y EDL-NH: principios de superposición y solución general

Teorema 20.7 (Principio de superposición, I)
Sean f y g dos soluciones de la ecuación en diferencias lineal homogénea de orden k,

$$c_0(n)h(n) + c_1(n)h(n-1) + c_2(n)h(n-2) + \cdots + c_k(n)h(n-k) = 0,$$

entonces para todo $\alpha, \beta \in \mathbb{R}$, $\alpha f + \beta g$ es también solución de dicha lineal homogénea.

Teorema 20.8 (Corolario)
Toda combinación lineal (finita) de soluciones de la ecuación en diferencias lineal homogénea de orden k es también solución de dicha ecuación.

[13] Sucesión A000292 en la OEIS, https://oeis.org/A000292.
[14] Sucesión A000332 en la OEIS, https://oeis.org/A000332.
[15] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Floyd%27s_triangle.
[16] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Bernoulli%27s_triangle.
[17] *Vid. v. gr.* https://en.wikipedia.org/wiki/Category:Triangles_of_numbers.

Teorema 20.9 (Principio de superposición, II)
Sea f una solución de la ecuación en diferencias lineal completa de orden k,

$$c_0(n)h(n) + c_1(n)h(n-1) + c_2(n)h(n-2) + \cdots + c_k(n)h(n-k) = F(n),$$

y sea g una solución de su homogénea asociada, entonces para todo $\beta \in \mathbb{R}$, $f + \beta g$ es también solución de dicha lineal completa.

Teorema 20.10 (Corolario)
La suma de una solución de la ecuación lineal completa de orden k con una combinación lineal (finita) de soluciones de su homogénea asociada es también solución de la lineal completa.

Esto se extiende a la situación general siguiente.

Definición 20.14.— Llamamos *sistema fundamental de soluciones* de la ecuación en diferencias lineal homogénea de orden k a un conjunto de k de sus soluciones $\{g_0, g_1, \dots, g_{k-1}\}$ tal que $\exists n_0 \in \mathbb{Z}$ tal que

$$\begin{vmatrix} g_0(n_0) & g_1(n_0) & \dots & g_{k-1}(n_0) \\ g_0(n_0-1) & g_1(n_0-1) & \dots & g_{k-1}(n_0-1) \\ \vdots & \vdots & \ddots & \vdots \\ g_0(n_0-k+1) & g_1(n_0-k+1) & \dots & g_{k-1}(n_0-k+1) \end{vmatrix} \neq 0.$$

Teorema 20.11 (Solución general)
Sea la ecuación en diferencias lineal completa de orden k,

$$c_0(n)h(n) + c_1(n)h(n-1) + c_2(n)h(n-2) + \cdots + c_k(n)h(n-k) = F(n),$$

y sea $\{g_0, g_1, \dots, g_{k-1}\}$ un sistema fundamental de soluciones de su homogénea asociada, entonces:

0. la *solución general de la lineal homogénea* es el conjunto infinito de funciones

$$\left\{ \sum_{i=0}^{k-1} \beta_i g_i ; \beta_0, \beta_1, \dots, \beta_{k-1} \in \mathbb{R} \right\};$$

1. la *solución general de la lineal completa* es el conjunto infinito de funciones

$$\left\{ f + \sum_{i=0}^{k-1} \beta_i g_i ; \beta_0, \beta_1, \dots, \beta_{k-1} \in \mathbb{R} \right\}.$$

A renglón seguido, desgranamos este resultado para el caso de coeficientes constantes, estudiando orden dos y general y homogeneidad frente a compleción.

§ 20.4.1 EDL-H-CC: polinomio característico y raíces características

A partir de aquí y con ánimo a familiarizarnos con lo que también es costumbre, notaremos $h(n+i)$ por h_{n+i}; igualmente, utilizaremos un nombre más frecuente en el ámbito de las sucesiones como es a_{n+i}. Más adelante, en problemas donde la variable dependiente sea el tiempo, notaremos y_{t+i}.

Dada la ecuación en diferencias lineal homogénea con coeficientes constantes de orden k

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0,$$

tratemos de hallar una solución que tenga la forma exponencial r^n ($r \neq 0$),

$$c_0 r^n + c_1 r^{n-1} + c_2 r^{n-2} + \cdots + c_{k-1} r^{n-k+1} + c_k r^{n-k} = 0,$$

esto es,

$$(c_0 r^k + c_1 r^{k-1} + c_2 r^{n-2} + \cdots + c_{k-1} r + c_k) r^{n-k} = 0,$$

lo que simplificando, queda

$$c_0 r^k + c_1 r^{k-1} + c_2 r^{n-2} + \cdots + c_{k-1} r + c_k = 0.$$

Definición 20.15.— Llamamos *polinomio característico* de la ecuación en diferencias al miembro izquierdo de esta última igualdad. Es de grado k y tiene, en general, k raíces, que llamamos *raíces características*. La propia igualdad se conoce como *ecuación característica* (o, sinónimamente, a veces, *ecuación auxiliar*) de la ecuación en diferencias). Las raíces características son las soluciones de esta ecuación.

§ 20.4.2 Resolución de una EDL-H-CC de orden dos

En este momento nos preocupa la resolución de una ecuación en diferencias lineal homogénea con coeficientes constantes, de orden dos.

Sean $c_0, c_1, c_2 \in \mathbb{R}$, la EDL homogénea con coeficientes constantes $c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0$ y su ecuación característica $c_0 r^2 + c_1 r + c_2 = 0$.

Distinguiremos dos casos según esta EDL tenga dos raíces características reales simples o una raíz característica real doble.

Caso de dos raíces reales simples

Así, por una parte, si tiene dos raíces reales distintas r_0 y r_1, cada una de ellas origina una solución particular de la ecuación en diferencias, a saber, las sucesiones $\{r_0^n\}$ y $\{r_1^n\}$, respectivamente —ha sido nuestro punto de partida, buscar soluciones con esta forma—.

En estas condiciones se satisface el siguiente teorema.

Teorema 20.12 (Teorema UNO)
La solución general de

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0$$

es la familia infinita de sucesiones $\{a_n\}$ definida por

$$a_n = c_{r_0} r_0^n + c_{r_1} r_1^n \ (c_{r_0}, c_{r_1} \in \mathbb{R}) .$$

Demostración.— Por el principio de superposición, ya que el conjunto $\{r_0^n, r_1^n\}$ es un sistema fundamental de soluciones. ■

Caso de una raíz real doble

Por la otra parte, si la EDL-H tiene una raíz real doble r_0, ésta origina dos soluciones particulares de la ecuación en diferencias, a saber, las sucesiones $\{r_0^n\}$ y $\{n r_0^n\}$.

En estas condiciones se satisface el siguiente teorema.

Teorema 20.13 (Teorema DOS)
La solución general de

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} = 0$$

es la familia infinita de sucesiones $\{a_n\}$ definida por

$$a_n = c_{r_{0,0}} r_0^n + c_{r_{0,1}} n r_0^n \ \left(c_{r_{0,0}}, c_{r_{0,1}} \in \mathbb{R}\right) .$$

Demostración.— Por el principio de superposición, ya que el conjunto $\{r_0^n, n r_0^n\}$ es un sistema fundamental de soluciones. ■

Ejemplo 732 (continuación del 646)

¿Cuántas palabras binarias de longitud siete existen que no contengan dos unos consecutivos?

[Cubit 156], [EFE 3.7.2024:14] (tipo test) (longitud n).

Resolución.— Pensemos ahora en un plateamiento con ecuaciones en diferencias. Para ello, notemos

$$\binom{n+1}{0}+\binom{n}{1}+\cdots+\binom{n-\lceil\frac{n}{2}\rceil+1}{\lceil\frac{n}{2}\rceil}$$

simplemente por $a(n)$, y tengamos bien presente que el significado de $a(n)$ es el número de palabras binarias de longitud n que no tienen dos unos consecutivos.

Para hallar la relación de recurrencia, consideremos el último bit de la palabra, entonces

0.º, si dicho bit es 0, hay $a(n-1)$ palabras que no tienen dos unos consecutivos, las correspondientes a la longitud de la subpalabra de los $n-1$ primeros bits, pues todos sus bits son libres de ser 0 o 1, ya que al ser un 0 el último bit de la palabra, éste no influye en que la palabra tenga dos unos consecutivos; por otro lado,

1.º, si el último bit de la palabra es 1, como no puede haber dos unos consecutivos, el bit anterior debe ser 0, por lo que son los $n-2$ primeros bits los que son libres de ser 0 o 1, esto es, hay $a(n-2)$ palabras que no tienen dos unos consecutivos.

Entonces, por el principio de la adición [¡esto requiere justificación! ✍],

$$a(n)=a(n-1)+a(n-2)$$

o escrita en otro formato para sucesiones,

$$a_n=a_{n-1}+a_{n-2}$$

siendo éste un ejemplo más de ecuación en diferencias, que como dijimos no es más que una expresión que relaciona un término cualquiera a_n, de una sucesión dada $\{a_n\}$, con uno o más términos anteriores o posteriores —*cfr. supra* definición 20.7 (pág. 1300 de esta edición)—. En el formato más tradicional de ecuaciones en diferencias lineales de orden k,

$$c_0(n)a_n+c_1(n)a_{n-1}+c_2(n)a_{n-2}+\cdots+c_k(n)a_{n-k}=F(n),$$

con $c_0, c_1, c_2, \ldots, c_k, F$ funciones en n, queda

$$a_n-a_{n-1}-a_{n-2}=0;$$

así, esta ecuación en diferencias es:

0. de orden 2, ya que $|0-2|=2$;
1. lineal, pues en los sumandos no aparecen productos de términos;
2. homogénea, porque en todos los sumandos aparece un término a_i, en otras palabras, F es la función constante nula, $F(n)=0$, con coeficientes constantes c_0, c_1, c_2 son funciones constantes $c_0(n)=c_0=1$, $c_1(n)=c_1=-1$, $c_2(n)=c_2=-1$.

Preocupémonos ahora por cómo resolver la ecuación en diferencias, lineal homogénea con coeficientes constantes y de orden 2,

$$a_n - a_{n-1} - a_{n-2} = 0 \tag{20.5}$$

Esto es, nuestro objetivo es encontrar una fórmula cerrada, una expresión explícita para a_n.

No es difícil comprobar que no se pliega telescópicamente. ¿Y qué hay de los métodos de sustitución, hacia adelante o hacia atrás? Pues que para esta sucesión, nada más que empezamos a intentarlo se nos complica bastante.

Es la hora de poner en práctica el cuarto método: coeficientes indeterminados.

Cómo resolver por este método una ecuación en diferencias lineal homogénea con coeficientes constantes, de orden 2, nos lo explica el teorema 20.12 (pág. 1314 de esta edición) (teorema UNO) y el teorema 20.13 (pág. 1314 de esta edición) (teorema DOS).

Lo primero es hallar las raíces características de (20.5), esto es, las soluciones de su ecuación característica

$$r^2 - r - 1 = 0,$$

que tiene dos soluciones reales distintas,

$$r_0 = \frac{1+\sqrt{5}}{2},$$
$$r_1 = \frac{1-\sqrt{5}}{2},$$

de donde, de acuerdo con el teorema 20.12 (pág. 1314 de esta edición) (teorema UNO), cualquier sucesión a_n que satisfaga (20.5) es de la forma

$$a_n = \rho_0 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + \rho_1 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n,$$

para determinados números reales ρ_0 y ρ_1.

Solución.— La solución general de (20.5) es

$$a_n = \rho_0 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + \rho_1 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n \qquad (\rho_0, \rho_1 \in \mathbb{R}) \tag{20.6}$$

lo cual significa que existe un número infinito no numerable de sucesiones a_n que son soluciones particulares de dicha ecuación, cada una de ellas determinada por dos valores reales concretos de ρ_0 y ρ_1. ■

Actividad 20.1

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición, mas es-

to requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Actividad 20.2

Para inferir la ecuación en diferencias, en vez de un *razonamiento regresivo*, hacia atrás, partiendo del bit final, bien pudiésemos haber hecho un *razonamiento progresivo*, hacia adelante, partiendo del bit inicial.

Observación 20.4.0.— Cualquier solución particular $\{a_n\}$ de (20.5) es de la forma (20.6), para dos números reales concretos ρ_0 y ρ_1; por ejemplo, si $\rho_0 = 1$ y $\rho_1 = 1$, se trata de los *números de* LUCAS[18], que corresponde al problema de valores iniciales

$$\begin{aligned} a_n - a_{n-1} - a_{n-2} &= 0 \quad (2 \leq n), \\ a_0 &= 2, \\ a_1 &= 1, \end{aligned}$$

y que en la OEIS está catalogada como la sucesión A000032[19].

De aquí en adelante, L_n significará el enésimo número de LUCAS, y su expresión, a la vez que definición, tradicional como problema de valores iniciales es

$$\begin{aligned} &L_n = L_{n-1} + L_{n-2} \quad (2 \leq n), \\ &L_0 = 2, \\ &L_1 = 1. \end{aligned}$$

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
L_n	2	1	3	4	7	11	18	29	47	76	...

Un segundo ejemplo: si $\rho_0 = 1/\sqrt{5}$ y $\rho_1 = -1/\sqrt{5}$, se trata de los *números de* FIBONACCI[20], que corresponde al problema de valores iniciales

$$\begin{aligned} a_n - a_{n-1} - a_{n-2} &= 0 \quad (2 \leq n), \\ a_0 &= 0, \\ a_1 &= 1; \end{aligned}$$

está catalogada como la sucesión A000045 en la OEIS[21].

[18] *Vid. v. gr.* https://es.wikipedia.org/wiki/Número_de_Lucas.
[19] *Vid.* https://oeis.org/A000032.
[20] *Vid. v. gr.* https://es.wikipedia.org/wiki/Sucesión_de_Fibonacci.
[21] *Vid.* https://oeis.org/A000045.

De aquí en adelante, F_n significará el enésimo número de FIBONACCI, y su expresión, a la vez que definición, tradicional como problema de valores iniciales es

$$F_n = F_{n-1} + F_{n-2} \quad (2 \leq n),$$
$$F_0 = 0,$$
$$F_1 = 1.$$

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
F_n	0	1	1	2	3	5	8	13	21	34	...

No es difícil demostrar que los números de LUCAS pueden definirse en función de los de FIBONACCI,

$$L_n = F_{n-1} + F_{n+1} \quad (1 \leq n),$$
$$L_0 = 2.$$

Observación 20.4.1.— La matriz $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ es conocida como la matriz Q de FIBONACCI. No es difícil demostrar —por inducción sobre n [✍]— que si $n \geq 1$, entonces

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

A partir de esto demostramos identidades, por ejemplo,

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_m F_n$$

(a partir de que $Q^{m+n} = Q^m Q^n$)), o la *identidad de* CASSINI,

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$$

(a partir de que $(-1)^n = |Q^n| = F_{n+1}F_{n-1} - F_n F_n$) (la demostraremos en el ejemplo 733 [pág. 1320 de esta edición] por inducción débil).

Por cierto, los números de FIBONACCI están presentes «por todas partes»[22].

[22] *Vid. v. gr.:*

- «Fibonacci está en todas partes» (Raúl IBÁÑEZ TORRES, en *Cuaderno de Cultura Científica*, 2024): Parte I (https://culturacientifica.com/2024/10/02/fibonacci-esta-en-todas-partes-i/), Parte II (https://culturacientifica.com/2024/10/16/fibonacci-esta-en-todas-partes-ii/) y Parte III (https://culturacientifica.com/2024/10/30/fibonacci-esta-en-todas-partes-y-iii/);
- «Nature by Numbers» —cortometraje inspirado en los números, la geometría y la naturaleza— (Cristóbal VILA, 2010) (https://etereaestudios.com/works/nature-by-numbers/), incluyendo esta página web información sobre la matemática subyacente a lo que aparece en dicho cortometraje —más trabajos de Cristóbal VILA, en su galería de trabajos de Etérea (https://etereaestudios.com/works/)—.

Observación 20.4.2.— Es posible definir los números de FIBONACCI mediante el siguiente sistema de LINDENMAYER (sistema L)[23]:

$$\Sigma = \{A, B\}$$ (alfabeto de L) [las únicas letras con las que formar palabras],

$$\Lambda = \{A\}$$ (axioma de L) [la palabra A, la única conocida al comienzo],

$$\mathcal{R} = \{R_{\mathrm{I}}, R_{\mathrm{II}}\}$$ (reglas de inferencia), donde estas reglas son:

Regla I: puede reemplazarse A por B en cualquier teorema.

Regla II: puede reemplazarse B por AB en cualquier teorema.

En formato de reglas, dadas cualesquiera dos fórmulas α y β,

$$R_{\mathrm{I}} : \frac{\alpha A \beta}{\alpha B \beta} \quad R_{\mathrm{II}} : \frac{\alpha B \beta}{\alpha AB \beta}.$$

A partir del axioma A y aplicando estas reglas, obtenemos la sucesión de palabras:

$$\begin{aligned} &A,\\ &B,\\ &AB,\\ &BAB,\\ &ABBAB,\\ &BABABBAB,\\ &ABBABBABABBAB,\\ &BABABBABABBABBABABBAB, \ldots \end{aligned}$$

en la que observamos que la sucesión de las longitudes de estas palabras son, precisamente, los números de FIBONACCI: 1, 1, 2, 3, 5, 8, 13, 21, . . .

Observación 20.4.3.— Incidentalmente, desde el punto de vista de las sucesiones, los números de FIBONACCI conforman una sucesión creciente, lejos del supercrecimiento de otras sucesiones[24].

Observación 20.4.4.— Utilizamos el artefacto en línea SageMath[25] y el siguiente programita en lenguaje Sage con un par de funciones recursivas para los números de FIBONACCI y LUCAS,

---

[23] *Vid. v. gr.* https://en.wikipedia.org/wiki/L-system, donde podemos apreciar su conexión con la *geometría fractal* (*vid. v. gr.* https://en.wikipedia.org/wiki/Fractal).

[24] Decimos que $\{a_n\}$ es una *sucesión supercreciente* si, y sólo si, satisface $\forall i \in \mathbb{N}$,

$$a_i \geq \sum_{j=0}^{i-1} a_j.$$

Es una *sucesión estrictamente supercreciente* si la desigualdad es estricta.

[25] *Cfr. supra* § 11 (pág. cii de esta edición).

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
def fibRec(n):
        if n < 2:
                return n
        else:
                return fibRec(n-1) + fibRec(n-2)
def lucRec(n):
        if n<1:
                return 2
        else:
                return fibRec(n-1) + fibRec(n+1)
print ([(fibRec(n),lucRec(n)) for n in range(12)])
```

para obtener (los devuelve e imprime) los doce primeros números de Fibonacci y Lucas, en las componentes inicial y final de los pares ordenados, respectivamente:

```
Share
[(0, 2), (1, 1), (1, 3), (2, 4), (3, 7), (5, 11), (8, 18), (13, 29), (21, 47), (34, 76), (55, 123), (89, 199)]
```

Observación 20.4.5.— En la observación 20.3.8 (pág. 1311 de esta edición) vimos cómo en el triángulo de Pascal (pág. 1130 de esta edición) aparecen sucesiones interesantes de números. Pues bien, cada número de Fibonacci, F_n, para $n \geq 1$, corresponde a una suma de los elementos de una diagonal nordeste de dicho triángulo, esto es, $\forall n \in \mathbb{Z}^+$,

$$F_n = \sum_{k=0}^{n-1} \binom{n-k-1}{k},$$

es decir, recorriendo dichas diagonales, $1 = 1 = F_1$, $1 = 1 = F_2$, $1+1 = 2 = F_3$, $1+2 = 3 = F_4$, $1+3+1 = 5 = F_5$, $1+4+3 = 8 = F_6$, $1+5+6+1 = 13 = F_7$, y así sucesivamente.

Ejemplo 733

Demostremos que $\forall n \in \mathbb{Z}^+$, $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$ (*identidad de* Cassini, 1680).

Resolución.— Demostrada en la observación 20.4.1 (pág. 1318 de esta edición) vía la matriz Q de Fibonacci, demostrémosla ahora por inducción débil. Notando «$F_{n-1}F_{n+1} = F_n^2 + (-1)^n$» por $P(n)$, lo que nos proponemos es demostrar que $\forall n \in \mathbb{Z}^+$, $P(n)$. Para ello, apliquemos el teorema 16.1 (pág. 806 de esta edición):

Caso base (ID$_0$).— Si $n = 1$, entonces $F_{1+1}F_{1-1} = 1 \cdot 0 = 0 = F_1^2 + (-1)^1$, de donde $P(1)$ es cierta.

Paso inductivo (ID$_1$).— Supongamos $P(k)$ y demostremos $P(k+1)$, esto es, supongamos que $F_{k-1}F_{k+1} = F_k^2 + (-1)^k$ (hipótesis de inducción) y demostremos que $F_kF_{k+2} = F_{k+1}^2 + (-1)^{k+1}$; en efecto, $F_kF_{k+2} = F_k(F_{k+1} + F_k)$ (por la recurrencia definitoria de F_n) $= F_kF_{k+1} + F_k^2 = F_kF_{k+1} + F_{k-1}F_{k+1} - (-1)^k$ [por hipótesis de inducción] $= F_kF_{k+1} + F_{k-1}F_{k+1} + (-1)^{k+1} =$

$(F_k + F_{k-1})F_{k+1} + (-1)^{k+1} = F_{k+1}F_{k+1} + (-1)^{k+1}$ [por la recurrencia definitoria de F_n] $= F_{k+1}^2 + (-1)^{k+1}$, esto es, $P(k+1)$.

Conclusión ($\text{ID}_0 \wedge \text{ID}_1$).— Como se satisfacen el caso base y el paso inductivo, entonces del teorema 16.1 (pág. 806 de esta edición) de inducción débil se sigue lo buscado, a saber, que $\forall n \in \mathbb{Z}^+, F_{n-1}F_{n+1} = F_n^2 + (-1)^n$. ■

Observación 20.4.6.— La *identidad de* CATALAN (1879),

$$F_n^2 - F_{n+m}F_{n-m} = (-1)^{n-m}F_m^2,$$

con $m \in \mathbb{Z}$, generaliza la identidad de CASSINI. La *identidad de* VAJDA (1960),

$$F_{n+i}F_{n+j} - F_nF_{n+i+j} = (-1)^n F_iF_j,$$

generaliza la identidad de CATALAN.[26]

Actividad 20.3

No sólo las vistas hasta este momento; a lo largo de los años se ha demostrado cómo los números de FIBONACCI satisfacen una gran cantidad de recurrencias. Sólo a modo de ejemplo, dos:

$$F_{2n} = 2F_{n-1}F_n + F_n^2,$$
$$F_{2n+1} = F_{n+1}^2 + F_n^2,$$

ambas si $2 \leq n$. Puede ser un buen ejercicio de computación escribir un procedimiento recursivo basado en estas dos y averiguar si este nuevo procedimiento incrementa la recomputación* con respecto al construido de acuerdo con la recurrencia definitoria de F_n, a saber, $F_n = F_{n-1} + F_{n-2}$ $(2 \leq n)$.

* Por recomputación nos referimos a que, por ejemplo, en el procedimiento definido a partir de la última recurrencia, el cálculo de F_{23} se hace a partir del cálculo de F_{22} y F_{21}, y que para hallar F_{22}, es necesario calcular F_{21} y F_{20} (como vemos, el cálculo de F_{21} se ha hecho dos veces —cosa que podría evitarse, por ejemplo, con una tabla auxiliar de memoria, pero no es el caso—).

Ejemplo 734 —continuación del ejemplo 732 (pág. 1314 de esta edición)—

¿Qué hay entonces de la respuesta a cuántas palabras binarias de longitud siete existen que no contengan dos unos consecutivos?

[Cubit 157].

[26] *Vid. v. gr.* https://en.wikipedia.org/wiki/Cassini_and_Catalan_identities.

Resolución.— Recordemos que la solución que hallamos fue 34 —*cfr. supra* ejemplo 646 (pág. 1176 de esta edición)—.

Asimismo, recordemos, una vez más, que en este ejemplo, a_n representa el número de palabras binarias de longitud n que no tienen dos unos consecutivos.

Como $a_n - a_{n-1} - a_{n-2} = 0$ es una ecuación en diferencias de orden 2, según el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), teniendo dos valores iniciales consecutivos, tenemos una solución particular.[27]

Así pues, necesitamos dos valores iniciales.

¿Qué sucede cuando $n = 0$? Es decir, $a_0 =$ ¿? (palabras de longitud 0; aunque estos argumentos por vacuidad nos siguen provocando dolor de cabeza, ¿verdad?). En cualquier caso, en el universo de las palabras el equivalente al conjunto vacío (conjunto sin elementos) es la palabra vacía, usualmente designada por ε, palabra sin letras y, por lo tanto, sin dos unos consecutivos, así que $a_0 = 1$. Sí nos parece claro que:

- $a_1 = 2$, porque ninguna de las dos únicas palabras de longitud uno posibles, a saber, 0 y 1, tiene dos unos consecutivos, y
- $a_2 = 3$, porque sólo las palabras 00, 01 y 10 son las que no tienen dos unos consecutivos (la palabra 11 sí que los tiene).

Aún más, son dos valores iniciales «adecuados» de acuerdo con el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), en el sentido de que son consecutivos y en número igual al orden de la ecuación, a saber, 2, así que la expresión explícita para $\{a_n\}$ es la única solución del problema de valores iniciales

$$\begin{aligned} a_n - a_{n-1} - a_{n-2} &= 0, \\ a_1 &= 2, \\ a_2 &= 3. \end{aligned}$$

Vamos a resolverlo. Sustituyendo cada valor inicial en la solución general (20.6),

$$a_n = \rho_0 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + \rho_1 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n \qquad (\rho_0, \rho_1 \in \mathbb{R}) \tag{20.7}$$

obtenemos el siguiente sistema de dos ecuaciones lineales con dos incógnitas ρ_0 y ρ_1:

$$(a_1 =)2 = \rho_0 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^1 + \rho_1 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^1,$$

[27] Precisamente esto es lo que ha ocurrido con los números de Fibonacci y Lucas —*cfr. supra* observación 20.4.0 (pág. 1317 de esta edición)—; observemos que la ecuación en diferencias es la misma, son los valores iniciales los que definen dichas sucesiones unívocamente.

$$(a_2 =)3 = \rho_0 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^2 + \rho_1 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^2,$$

cuya solución es

$$\rho_0 = \frac{1+\frac{3}{\sqrt{5}}}{2},$$
$$\rho_1 = \frac{1-\frac{3}{\sqrt{5}}}{2},$$

esto es, la expresión explícita (fórmula cerrada) para a_n es

$$a_n = \frac{1+\frac{3}{\sqrt{5}}}{2} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n + \frac{1-\frac{3}{\sqrt{5}}}{2} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Solución.— Pues sí, en efecto, la respuesta a la pregunta «¿cuántas palabras binarias de longitud siete existen que no contengan dos unos consecutivos?» es 34:

$$a_7 = \frac{1+\frac{3}{\sqrt{5}}}{2} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^7 + \frac{1-\frac{3}{\sqrt{5}}}{2} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^7$$
$$= 34.$$

■

Observación 20.4.7.— Es posible expresar a_n en función de los números de Fibonacci:

$$a_n = F_{n+2}.$$

De hecho, se menciona en la OEIS al comienzo de la página correspondiente: «$F(n+2)$ = número de secuencias binarias de longitud n que no tienen ceros consecutivos»[28] (notemos que da igual interpretar con 0 o con 1; se trata de cadenas binarias, cadenas de dos símbolos x e y, sean éstos los que sean)). (Si tenemos inquietud y disponemos de tiempo, observemos además la profusión de interpretaciones que aparecen en los comentarios).

[Cubit 158].

Observación 20.4.8.— Claro que también es posible expresar a_n en función de los números de Fibonacci y Lucas:

$$a_n = \frac{3F_n + L_n}{2}.$$

De hecho, si solicitamos al artefacto en línea Wolfram|Alpha la solución de nuestro problema de valores iniciales, introduciendo `solve a(n) = a(n-1) + a(n-2), a(1) = 2, a(2) = 3`, ésa es su respuesta.

---

[28] *Vid.* https://oeis.org/A000045.

[Cubit 159].

Observación 20.4.9.— Utilizamos el artefacto en línea SageMath[29] y este programita en lenguaje Sage (no olvidemos que es un buen ejercicio el inferir la lógica subyacente, en otras palabras, anotar cada línea de código),

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
def str_no11(n):
        str_k = ['0','1']
        tmp = []
        for k in [2..n]:
                for c in str_k:
                        tmp.append(c+'0')
                        if c[-1] == '0':
                                tmp.append(c+'1')
                str_k = tmp[:]
                tmp = []
        return str_k
str_no11(7)
```

para obtener las 34 palabras de siete bits que no contienen dos unos consecutivos, solución del ejemplo:

```
['0000000', '0000001', '0000010', '0000100', '0000101', '0001000', '0001001', '0001010', '0010000',
'0010001', '0010010', '0010100', '0010101', '0100000', '0100001', '0100010', '0100100', '0100101',
'0101000', '0101001', '0101010', '1000000', '1000001', '1000010', '1000100', '1000101', '1001000',
'1001001', '1001010', '1010000', '1010001', '1010010', '1010100', '1010101']
```

Observación 20.4.10.— Recordemos que el enésimo número de FIBONACCI, F_n, se expresa, a la vez que se define, como el problema de valores iniciales

$$
\begin{aligned}
&F_n = F_{n-1} + F_{n-2} \quad (2 \leq n),\\
&F_0 = 0,\\
&F_1 = 1.
\end{aligned}
$$

Vía un desarrollo similar al hecho en el ejemplo anterior, obtuviésemos que su fórmula explícita es

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n,$$

expresión que podemos simplificar usando el número áureo,

$$\varphi = \frac{1+\sqrt{5}}{2},$$

[29] *Cfr. supra* § 11 (pág. cii de esta edición).

y como $\varphi^{-1} = \varphi - 1$, queda

$$F_n = \frac{\varphi^n - (-\varphi^{-1})^n}{\sqrt{5}},$$

que es conocida como *fórmula de* BINET (aunque es atribuida a Édouard LUCAS).

Actividad 20.4

[(accesoria)] Conozcamos el *árbol de* FIBONACCI. Un par de referencias iniciales pudiesen ser el artículo «El árbol de Fibonacci», de Raúl IBÁÑEZ, publicado el 20.3.2024 en *Cuaderno de Cultura Científica* (disponible en: https://culturacientifica.com/2024/03/20/el-arbol-de-fibonacci/) y el libro *Algoritmos + Estructuras de Datos = Programas*, de Niklaus WIRTH.

§ 20.4.3 Resolución de una EDL-H-CC de orden k

Sean $c_0, c_1, c_2, \cdots, c_k \in \mathbb{R}$, la EDL homogénea con coeficientes constantes $c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0$ y su ecuación característica $c_0 r^k + c_1 r^{k-1} + c_2 r^{n-2} + \cdots + c_{k-1} r + c_k = 0$.

Distinguiremos dos casos según esta EDL tenga k raíces características reales simples, esto es, el mismo número que el orden de la EDL, o tenga t raíces características reales múltiples.

Caso de raíces características reales simples

Nos interesa la resolución de una ecuación en diferencias lineal homogénea con coeficientes constantes, de orden k y con k raíces características reales simples, esto es, suponemos que la EDL tiene k raíces características reales distintas $r_0, r_1, \ldots, r_{k-1}$. Pues bien, cada una de estas raíces origina una solución particular de la ecuación en diferencias, a saber, las sucesiones $\{r_0^n\}$, $\{r_1^n\}$, …, $\{r_{k-1}^n\}$.

En estas condiciones tenemos el siguiente teorema.

Teorema 20.14 (Teorema TRES)
(Es una generalización del teorema UNO). La solución general de

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0,$$

siendo ésta tal que tiene k raíces características reales simples, es la familia infinita de sucesiones $\{a_n\}$ definida por

$$a_n = c_{r_0} r_0^n + c_{r_1} r_1^n + \cdots + c_{r_{k-1}} r_{k-1}^n \ (c_{r_0}, c_{r_1}, \ldots, c_{r_{k-1}} \in \mathbb{R}).$$

Demostración.— Por el principio de superposición, ya que $\{r_0^n, r_1^n, \ldots, r_{k-1}^n\}$ es un sistema fundamental de soluciones. ■

Caso de raíces características reales múltiples

Nos interesa ahora la resolución de una ecuación en diferencias lineal homogénea con coeficientes constantes, de orden $\boldsymbol{k}$ y con $\boldsymbol{t}$ raíces características reales múltiples. Suponemos entonces que la EDL tiene t raíces características reales $r_0, r_1, \ldots, r_{t-1}$ con multiplicidades respectivas $m_0, m_1, \ldots, m_{t-1}$, siendo $m_0 + m_1 + \cdots + m_{t-1} = k$. Pues bien, cada raíz r_i con multiplicidad $m_i > 1$ origina m_i soluciones particulares de la ecuación en diferencias, a saber, las sucesiones $\{r_i^n\}, \{nr_i^n\}, \{n^2 r_i^n\}, \ldots, \{n^{m_i-1} r_i^n\}$.

Imaginemos que r_i fuese la única con multiplicidad mayor que 1, entonces, por el principio de superposición, la sucesión $\{a_n\}$ definida por

$$\begin{aligned} a_n = {} & c_{r_0} r_0^n + c_{r_1} r_1^n \\ & + \cdots \\ & + c_{r_{i,0}} r_i^n + c_{r_{i,1}} n r_i^n + c_{r_{i,2}} n^2 r_i^n + \ldots + c_{r_{i,m_i-1}} n^{m_i-1} r_i^n \\ & + \cdots \\ & + c_{r_{k-1}} r_{k-1}^n, \end{aligned}$$

esto es, por

$$\begin{aligned} a_n = {} & c_{r_0} r_0^n + c_{r_1} r_1^n \\ & + \cdots \\ & + \left(c_{r_{i,0}} + c_{r_{i,1}} n + c_{r_{i,2}} n^2 + \cdots + c_{r_{i,m_i-1}} n^{m_i-1} \right) r_i^n \\ & + \cdots \\ & + c_{r_{k-1}} r_{k-1}^n, \end{aligned}$$

con $c_{r_0}, \ldots, c_{r_{i-1}}, c_{r_{i,0}}, \ldots, c_{r_{i,m_i-1}}, c_{r_{i+1}}, \ldots, c_{r_{k-1}} \in \mathbb{R}$, sería la solución general de la ecuación en diferencias.

Así, llegamos al siguiente teorema.

Teorema 20.15 (Teorema CUATRO)
(Es una generalización del teorema DOS). La solución general de

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0,$$

siendo ésta tal que tiene t raíces características reales $r_0, r_1, \ldots, r_{t-1}$ ($t < k$) con multiplicidades respectivas $m_0, m_1, \ldots, m_{t-1}$ (siendo $m_0 + m_1 + \cdots + m_{t-1} = k$), es la familia infinita de sucesiones $\{a_n\}$ definida por

$$\begin{aligned} a_n = {} & \left(c_{r_{0,0}} + c_{r_{0,1}} n + c_{r_{0,2}} n^2 + \cdots + c_{r_{0,m_0-1}} n^{m_0-1}\right) r_0^n \\ & + \left(c_{r_{1,0}} + c_{r_{1,1}} n + c_{r_{1,2}} n^2 + \cdots + c_{r_{1,m_1-1}} n^{m_1-1}\right) r_1^n \\ & + \cdots \\ & + \left(c_{r_{t-1,0}} + c_{r_{t-1,1}} n + c_{r_{t-1,2}} n^2 + \cdots + c_{r_{t-1,m_{t-1}-1}} n^{m_{t-1}-1}\right) r_{t-1}^n, \end{aligned}$$

con $c_{r_{i,j}} \in \mathbb{R}$, para $0 \leq i \leq t-1$ y $0 \leq j \leq m_{i-1} - 1$.

Demostración.— Por el principio de superposición, ya que

$$\{r_0^n, nr_0^n, n^2 r_0^n, \ldots, n^{m_0-1} r_0^n, \ldots, r_{t-1}^n, nr_{t-1}^n, n^2 r_{t-1}^n, \ldots, n^{m_{t-1}-1} r_{t-1}^n\}$$

es un sistema fundamental de soluciones. ■

§ 20.4.4 Resolución de una EDL-NH-CC

Sean $c_0, c_1, c_2, \cdots, c_k \in \mathbb{R}$, la EDL no homogénea con coeficientes constantes

$$c_0(n) a_n + c_1(n) a_{n-1} + c_2(n) a_{n-2} + \cdots + c_k(n) a_{n-k} = F(n), \tag{20.8}$$

y su homogénea asociada

$$c_0(n) a_n + c_1(n) a_{n-1} + c_2(n) a_{n-2} + \cdots + c_k(n) a_{n-k} = 0. \tag{20.9}$$

Obtención de la solución general

Suponiendo que conocemos una solución particular $\{a_n^{(p)}\}$ de la EDL-NH-CC y la solución general $\{a_n^{(h)}\}$ de su homogénea asociada, se tiene el siguiente teorema.

Teorema 20.16 (Teorema CINCO)
La solución general de la EDL-NH-CC (20.8) es la suma de las anteriores, esto es,

$$\{a_n^{(p)}\} + \{a_n^{(h)}\}.$$

Aún más, la suma de una solución de la EDL-NH-CC y de una solución de la EDL-H-CC es solución de la EDL-NH-CC.

Obtención de una solución particular

Falta que aprendamos a hallar $\{a_n^{(p)}\}$.

Se trata ahora, pues, de obtener una solución particular de una ecuación en diferencias lineal no homogénea con coeficientes constantes, de orden $\boldsymbol{k}$.

Este método supone que una solución particular de la no homogénea tiene la forma del término no homogéneo $F(n)$. Sólo consideraremos el caso en el que es de la forma

$$F(n) = \left(b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0\right) s^n, \tag{20.10}$$

con $b_t, b_{t-1}, \cdots, b_1, b_0, s \in \mathbb{R}$, esto es, cuando $F(n)$ es el producto de un polinomio en n por la enésima potencia de una constante, lo cual incluye los casos en los que $F(n)$ es un polinomio o $F(n)$ es una función potencia.

En estas condiciones tenemos el siguiente teorema.

Teorema 20.17 (Teorema SEIS)
Si s no es una raíz característica de la homogénea asociada a la EDL-NH-CC (20.8), entonces existe una solución particular de la no homogénea de la forma

$$\left(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0\right) s^n,$$

mientras que si sí lo es, con multiplicidad m_s, existe una solución particular de la no homogénea de la forma

$$n^{m_s}\left(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0\right) s^n,$$

con $p_t, p_{t-1}, \cdots, p_1, p_0, s \in \mathbb{R}$.

§ 20.4.5 Síntesis: algoritmo de resolución en cinco pasos (ARED5)

Para la solución de problemas de valores iniciales de ecuaciones en diferencias lineales con coeficientes constantes, siendo el término no homogéneo $F(n)$ el producto de un polinomio en n por la potencia enésima de una constante, es posible sintetizar el método de coeficientes indeterminados en un procedimiento consistente en cinco pasos.

Consideramos, pues, el problema de valores iniciales de orden k,

$$\begin{cases} c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = F(n), \\ a_0 = v_0, a_1 = v_1, \ldots, a_{k-1} = v_{k-1}, \end{cases}$$

donde $v_0, v_1, \ldots, v_{k-1} \in \mathbb{R}$ son los valores iniciales y $F(n)$ el producto de un polinomio en n por la potencia enésima de una constante, esto es,

$$F(n) = \left(b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0\right) s^n.$$

Para resolver este PVI, procederemos en cinco pasos.

Paso I.

Obtención de las raíces características de la ecuación en diferencias.

Considéremos la homogénea asociada,

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0,$$

y obtengamos su ecuación característica,

$$c_0 r^k + c_1 r^{k-1} + c_2 r^{n-2} + \cdots + c_{k-1} r + c_k = 0;$$

finalmente, solucionémosla, esto es, hallemos las raíces características de la ecuación en diferencias.

Paso II.

Obtención de la solución general de la homogénea asociada.

Cada raíz característica simple r genera un término de la forma —*cfr. supra* teorema 20.12 (pág. 1314 de esta edición) (teorema UNO) y teorema 20.14 (pág. 1325 de esta edición) (teorema TRES)—

$$c_r r^n,$$

y cada raíz característica múltiple r de multiplicidad m_r, genera los términos —*cfr. supra* teorema 20.13 (pág. 1314 de esta edición) (teorema DOS) y teorema 20.15 (pág. 1327 de esta edición) (teorema CUATRO)—

$$c_{r_0} r^n, c_{r_1} n r^n, c_{r_2} n^2 r^n, \ldots, c_{r_{m_r-1}} n^{m_r-1} r^n.$$

Determinaremos posteriormente las constantes $c_r, c_{r_0}, c_{r_1}, \ldots, c_{r_{m_r-1}} \in \mathbb{R}$. La solución general de la homogénea asociada $\{a_n^{(h)}\}$ es la suma de todos los términos generados por todas las raíces características. Si $F(n) = 0$, debemos ir al paso 4 con 0 como la solución particular de la no homogénea.

Paso III.

Obtención de una solución particular de la no homogénea.

Consideremos la forma general

$$F(n) = \left(b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0\right) s^n,$$

con $b_t, b_{t-1}, \cdots, b_1, b_0, s \in \mathbb{R}$ (por ejemplo: $F(n) = 2 \cdot 3^n$, $b_0 = 2$, $s = 3$; $F(n) = 3^{n-2}$, $b_0 = 1 \cdot 3^{-2}$, $s = 3$) y procedamos según lo establecido en el teorema 20.17 (pág. 1328 de esta edición) (teorema SEIS) para obtener $\{a_n^{(p)}\}$.

Paso IV.

Obtención de la solución general de la no homogénea.

Es la suma de la solución general de la homogénea asociada $\{a_n^{(h)}\}$ (obtenida en el paso 2) más la solución particular de la no homogénea $\{a_n^{(p)}\}$ (siendo ésta 0 si $F(n) = 0$, o la obtenida en el paso 3) —*cfr. supra* teorema 20.16 (pág. 1328 de esta edición) (teorema CINCO)—.

Paso V.

Obtención de la solución del problema de valores iniciales.

La sustitución de cada valor inicial en la solución general de la no homogénea nos proporciona una ecuación lineal con las constantes desconocidas como incógnitas. Al solucionar el sistema resultante de ecuaciones lineales, obtenemos los valores de estas constantes. Finalmente, la sustitución de estos valores en la solución general de la no homogénea, nos proporciona, en forma explícita, la única solución del problema de valores iniciales —*cfr. supra* teorema 20.17 (pág. 1328 de esta edición) (teorema SEIS)—.

Observación 20.4.11.— En estas notas sólo trabajamos con raíces reales; si nos interesase saber cómo trabajar con raíces complejas, pudiésemos acudir a la bibliografía recomendada[30].

§ 20.5 Muestra de ejemplos

Para los ejemplos siguientes, utilicemos la teoría de ecuaciones en diferencias para, en todos los casos razonando su porqué, modelizar y resolver la situación expuesta en la cuestión en estudio: I, propongamos una ecuación en diferencias (ED) o más; II, propongamos un problema de valores iniciales (PVI); III, demostremos que dicho PVI tiene solución única; IV, calculemos las raíces características pertinentes; V, obtengamos las soluciones de las ED concernientes, y VI, resolvamos el mencionado PVI y, por tanto, obtengamos la solución explícita de la cuestión.

[30] *Cfr. infra* § 20.9 (pág. 1421 de esta edición).

§ 20.5.0 EDLCC homogéneas

Ejemplo 735

Demostremos que el número de subconjuntos de un conjunto de n elementos es 2^n.

[Cubit 161].

Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más.*

Cuando añadimos un elemento a un conjunto, éste dobla el número de sus subconjuntos, pues todo subconjunto previo sigue siéndolo (cuyo número es a_{n-1}) y los nuevos subconjuntos se obtienen como unión del nuevo elemento con cada subconjunto previo (por lo que el número de nuevos subconjuntos también es a_{n-1}).

Propondremos una ecuación en diferencias a partir del principio de adición. Sean los sucesos: $S \leftrightharpoons$ ser subconjunto de un conjunto de n elementos; $S_0 \leftrightharpoons$ ser subconjunto de un conjunto de $n-1$ elementos (llamémoslo subcnjunto «original»); $S_1 \leftrightharpoons$ ser un subconjunto unión de un nuevo elemento con un subconjunto original. Claramente, S_0 y S_1 son incompatibles y $S = S_0 \cup S_1$. Por el principio de la adición, el número de formas en que sucede S, $\#S$, número que llamamos a_n, es igual a $\#S_0$ (a_{n-1}) más $\#S_1$ (a_{n-1}).

Reflejamos esto con la ecuación en diferencias

$$a_n = 2a_{n-1} \qquad (1 \leq n). \tag{20.11}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Por otro lado, el conjunto vacío, aun sin elementos, tiene un subconjunto, a saber, él mismo. Esto se traduce en la condición inicial $a_0 = 1$.

Es por ello que la situación se recoge en el PVI

$$\begin{aligned} a_n &= 2a_{n-1} \qquad (1 \leq n), \\ a_0 &= 1. \end{aligned}$$

III. *Demostración de que dicho PVI tiene solución única.*

La ecuación en diferencias $a_n - 2a_{n-1} = 0$ es de orden uno, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, *tiene una única solución* (también conocida como expresión explícita).

IV. *Cálculo de las raíces características pertinentes*. Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es

$$r - 2 = 0, \tag{20.12}$$

tiene una raíz real simple (con multiplicidad uno),

$$r_0 = 2. \tag{20.13}$$

V. *Obtención de las soluciones de las ED concernientes*.

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De lo anterior, de acuerdo con el teorema 20.14 (pág. 1325 de esta edición) (teorema TRES), cualquier sucesión $\{a_n\}$ que satisfaga (20.11) es de la forma

$$a_n = \rho_0 \cdot 2^n, \tag{20.14}$$

para un cierto número real ρ_0.

En otras palabras, $\{a_n\}$ definida por $a_n = \rho_0 \cdot 2^n$, donde $\rho_0 \in \mathbb{R}$, es la solución general de (20.11), lo cual significa que existe un número infinito no numerable de sucesiones $\{a_n\}$ que son soluciones particulares de (20.11), cada una de ellas determinada por un valor real concreto de ρ_0.

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo el valor inicial en la solución general (20.14), obtenemos la ecuación lineal con una incógnita ρ_0,

$$(a_0 =)1 = \rho_0 \cdot 2^0$$

cuya única solución es $\rho_0 = 1$.

En definitiva, una expresión explícita para $\{a_n\}$ es

$$a_n = 2^n \qquad (n \in \mathbb{N}).$$



Observación 20.5.0.— Ésta es la *sucesión de las potencias de dos*[31].

Observación 20.5.1.— Está catalogada como la sucesión A000079 en la OEIS[32].

Observación 20.5.2.— Pudiésemos utilizar el artefacto en línea SageMath[33] y este programita en lenguaje Sage para definir el polinomio característico de una ecuación en diferencias lineal homogénea con coeficientes constantes de orden k

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0,$$

mediante la función

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
def charpoly(constants):
        k = len(constants) - 1
        return constants[0]*x^k + sum([constants[i+1]*x^(k-i-1) for i in range(k)])
```

para, por ejemplo, ver la ecuación característica, que en este caso, como la ecuación en diferencias es $a_n - 2a_{n-1} = 0$, es

```
show(charpoly([1,-2]) == 0)
```

y calcular y mostrar las raíces características de la ED, en este ejemplo,

```
charroots = [charp[0] for charp in charpoly([1,-2]).roots()]
for r in charroots:
        show(r)
```

Actividad 20.5

Repasemos todas las formas en las que en estas notas, hasta ahora, hemos demostrado que el cardinal del conjunto potencia de un conjunto de cardinal n es 2^n.

[Cubit 162].

[31] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Potencia_de_dos.
[32] *Vid.* https://oeis.org/A000079.
[33] *Cfr. supra* § 11 (pág. cii de esta edición).

Ejemplo 736

Se lanza n veces una moneda al aire, ¿en cuántos resultados posibles (sucesos elementales) no aparecen dos caras consecutivas? —Por ejemplo, si $n = 2$, son tres: $\langle$cara, cruz$\rangle$, $\langle$cruz, cara$\rangle$, $\langle$cruz, cruz$\rangle$.

[EFO 17.1.2022:10], [EFEC 29.1.2025:14] (tipo test). *Cfr.* AGUADO, GAGO, LADRA, PÉREZ, VIDAL y VIEITES [213]: ejercicio 6.9 (págs. 135–136).

Resolución.— Esta cuestión es equivalente a la estudiada en el ejemplo 734 (pág. 1321 de esta edición).

I. *Propuesta de una ecuación en diferencias (ED) o más.*

En efecto, si sale cruz la primera vez, hay a_{n-1} resultados posibles de no aparecer dos caras consecutivas en los próximos $n-1$ lanzamientos; si sale cara la primera vez, la segunda deberá salir cruz, por lo que hay a_{n-2} resultados posibles de no aparecer dos caras consecutivas en los siguientes $n-2$ lanzamientos. Luego, como en el ejemplo estudiado,

$$a_n = a_{n-1} + a_{n-2} \qquad (3 \leq n).$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Además:

- $a_1 = 2$, pues en el lanzamiento de una moneda hay dos casos en el que no aparecen dos caras consecutivas, a saber, bien sale cara, bien sale cruz;
- $a_2 = 3$, como se ha comentado en el enunciado.

En definitiva, que esta cuestión es equivalente a la estudiada en el ejemplo 734 (pág. 1321 de esta edición). A él remitimos para ver la resolución detallada de los apartados III, IV, V y VI.

Solución.— Si se lanza n veces una moneda al aire, el número de resultados posibles (sucesos elementales) en los que no aparecen dos caras consecutivas es a_n que, expresado en función de los números de FIBONACCI, es

$$a_n = F_{n+2} \qquad (n \in \mathbb{Z}^+).$$



Ejemplo 737

Calculemos cuántas palabras ternarias (base 3) de longitud n no tienen dos cifras consecutivas iguales.

[EFO 4.6.2021:9], [EFEC 29.1.2025:13] (tipo test).

Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más.*

Sea a_n el número buscado. Sea una palabra válida de longitud n. Como su última cifra debe ser distinta de su penúltima cifra, ésta sólo tiene dos posibles valores (los dos valores distintos de su última cifra —trabajamos en base 3—), por lo que, por el principio de la adición [¡esto requiere justificación! ✍], $a_n = a_{n-1} + a_{n-1}$, en definitiva,

$$a_n - 2a_{n-1} = 0 \tag{20.15}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Al ser la ecuación lineal homogénea de coeficientes constantes y orden 1, por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), basta con un valor inicial para conformar un problema de valores iniciales de ecuaciones en diferencias que tenga una solución única. Exploramos posibles valores iniciales:

$a_0 = 1$ (la palabra vacía);

$a_1 = 3$ (las palabras 0, 1 y 2);

$a_2 = 6$ (las palabras 01, 02, 10, 12, 20 y 21).

Observamos que (20.15) representa la cuestión en estudio para $n > 1$ (esto es, $a_0 = 1$ es un caso ajeno a la recurrencia), es decir, que la sucesión que buscamos tiene como definición implícita:

$$\begin{aligned} a_n - 2a_{n-1} &= 0 \qquad (n > 1) \\ a_0 &= 1 \\ a_1 &= 3 \end{aligned}$$

Así, con $a_1 = 3$ conformamos *el problema de valores iniciales* que resolveremos con la teoría estudiada:

$$\begin{aligned} a_n - 2a_{n-1} &= 0 \qquad (n > 1) \\ a_1 &= 3 \end{aligned}$$

III. *Demostración de que dicho PVI tiene solución única.*

Se trata de una ecuación en diferencias de orden 1, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, *tiene una única solución*.

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (la propia ED original en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED (20.15) es $r-2$, siendo $r_0 = 2$ su única raíz característica, real y simple (multiplicidad 1).

V. *Obtención de las soluciones de las ED concernientes.*

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De lo anterior, por un teorema conocido —*cfr. supra* teorema 20.15 (pág. 1327 de esta edición) (teorema CUATRO)—, *la solución general* es

$$a_n = c_{r_0} 2^n \qquad (c_{r_0} \in \mathbb{R}). \tag{20.16}$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

VI. *Obtención de la solución del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Para ello, como es una ecuación de orden 1, se necesita un valor inicial, en este caso, $a_1 = 3$. Así:

$$a_1 = 3 = c_{r_0} 2^1,$$

de donde:

$$c_{r_0} = \frac{3}{2}. \tag{20.17}$$

Sustituyendo (20.17) en (20.16), obtenemos el número buscado $a_n = \frac{3}{2} 2^n$ (para $n > 0$).

Solución.— El número de palabras ternarias de longitud n que no tienen dos cifras consecutivas iguales es

$$a_n = 3 \cdot 2^{n-1} \qquad (n > 0)$$
$$a_0 = 1$$



Actividad 20.6

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Observación 20.5.3.— La sucesión $\{a_n\}$ está catalogada como la sucesión A003945 en la OEIS[34], donde encontramos más fórmulas e interpretaciones.

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
a_n	1	3	6	12	24	48	96	192	384	768	...

Observación 20.5.4.— Una vez resuelto I, esto es, obtenido el problema de valores iniciales de ecuaciones en diferencias y demostrado que tiene solución única, pudiésemos haberlo solucionado por cualquier otro método estudiado o conocido, sin olvidar que en algunos casos, como por ejemplo, si lo hubiésemos hecho mediante expansión, deberíamos demostrar el resultado seguramente mediante inducción. En nuestra resolución no hace falta, pues el resultado es consecuencia de la aplicación directa de teoremas (y no de una intuición).

Ejemplo 738

Siendo n un número natural, calculemos el número de subconjuntos de $\{1, 2, \dots, n\}$ que no contienen números consecutivos.

[EFE 7.7.2021:9], [EFEC 29.1.2025:15] (tipo test). *Cfr.* AGUADO, GAGO, LADRA, PÉREZ, VIDAL y VIEITES [213]: ejercicio 6.10 (pág. 136).

Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más*.

Designemos a_n para representar el número de subconjuntos buscado. Para construir una ecuación en diferencias para a_n, razonemos hacia atrás, dado un subconjunto S de $\{1, 2, \dots, n\}$ que no contiene números consecutivos, hay dos casos, según pertenezca o no n a S:

[34] *Vid*. https://oeis.org/A003945.

0. si n no pertenece a S, se trata en realidad de un subconjunto de $\{1, \ldots, n-1\}$ y hay a_{n-1} de éstos;

1. si n pertenece a S, como S no contiene números consecutivos, $n-1$ no pertenece a S y contar cuántos hay es tan sencillo como quitar n de ellos n, pues al no estar ni n ni $n-1$, su número es a_{n-2}.

Subyace el *principio de la adición*. Estos casos (sucesos, en realidad) se excluyen mutuamente (son incompatibles, ya que n, bien pertenece a S, bien no pertenece a S) y su unión es el suceso ser subconjunto de $\{1, 2, \ldots, n\}$ sin números consecutivos, entonces, por el principio de la adición, dicho suceso unión sucede de $a_n = a_{n-1} + a_{n-2}$ formas distintas, en definitiva,

$$a_n - a_{n-1} - a_{n-2} = 0. \tag{20.18}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Al ser la ecuación lineal homogénea de coeficientes constantes y orden 2, por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), basta con un valor inicial para conformar un problema de valores iniciales de ecuaciones en diferencias que tenga una solución única. Exploramos posibles valores iniciales:

$a_0 = 1$ (con 0 elementos, sólo hay un conjunto, el vacío);

$a_1 = 2$ (con 1 elemento, hay dos, el vacío y el propio conjunto).

Observamos, pues, que la sucesión que buscamos tiene como definición implícita *el problema de valores iniciales de ecuaciones en diferencias*

$$\begin{aligned} a_n - a_{n-1} - a_{n-2} &= 0 \qquad (n > 2) \\ a_0 &= 1 \\ a_1 &= 2. \end{aligned}$$

III. *Demostración de que dicho PVI tiene solución única.*

Se trata de una ecuación en diferencias de orden 2, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, *tiene una única solución*.

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio caracte-

rístico asociado a dicha ED es

$$x^2 - x - 1,$$

siendo

$$r_0 = \frac{-(-1) - \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-1)}}{2 \cdot 1} = \frac{1 - \sqrt{5}}{2},$$
$$r_1 = \frac{-(-1) + \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-1)}}{2 \cdot 1} = \frac{1 + \sqrt{5}}{2},$$

las raices características distintas y simples (esto es, ambas con multiplicidad uno) de dicha ED.

v. *Obtención de las soluciones de las ED concernientes*.

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De lo anterior que por un teorema conocido —teorema 20.12 (pág. 1314 de esta edición) (teorema UNO) o teorema 20.15 (pág. 1327 de esta edición) (teorema CUATRO)— *la solución general* es:

$$a_n = c_{r_0} \left(\frac{1 - \sqrt{5}}{2} \right)^n + c_{r_1} \left(\frac{1 + \sqrt{5}}{2} \right)^n \qquad (c_{r_0}, c_{r_1} \in \mathbb{R}). \tag{20.19}$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

vi. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo los dos valores iniciales consecutivos en la solución general obtenida,

$$(a_0 =)1 = c_{r_0} \left(\frac{1 - \sqrt{5}}{2} \right)^0 + c_{r_1} \left(\frac{1 + \sqrt{5}}{2} \right)^0,$$
$$(a_1 =)2 = c_{r_0} \left(\frac{1 - \sqrt{5}}{2} \right)^1 + c_{r_1} \left(\frac{1 + \sqrt{5}}{2} \right)^1,$$

de donde,

$$c_{r_0} = \frac{5 - 3\sqrt{5}}{10}, \tag{20.20}$$
$$c_{r_1} = \frac{5 + 3\sqrt{5}}{10}. \tag{20.21}$$

Sustituyendo (20.20) y (20.21) en (20.19), obtenemos el número buscado

$$a_n = \frac{5-3\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^n + \frac{5+3\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n.$$

Solución.— El número de subconjuntos de $\{1, 2, \dots, n\}$ sin números consecutivos viene dado por

$$a_n = \frac{5-3\sqrt{5}}{10}\left(\frac{1-\sqrt{5}}{2}\right)^n + \frac{5+3\sqrt{5}}{10}\left(\frac{1+\sqrt{5}}{2}\right)^n \qquad (n \geq 0).$$ ■

Observación 20.5.5.— Para todo n natural,

$$a_n = F_{n+2},$$

donde $\{F_n\}$ es la sucesión de FIBONACCI, catalogada como la sucesión A000045 en la OEIS[35], donde encontramos diversas fórmulas e interpretaciones, por ejemplo, referidas a esta cuestión, lo que hemos demostrado, que F_{n+2} es el «número de subconjuntos de $\{1, 2, \dots, n\}$ que no contienen enteros consecutivos» y también, en relación a lo que discutiremos a continuación, en la observación 20.5.6 (pág. 1340 de esta edición), el «número de palabras binarias de longitud n que no tienen ceros consecutivos».

n	0	1	2	3	4	5	6	7	8	9	...
a_n	1	2	3	5	8	13	21	34	55	89	...
F_n	0	1	1	2	3	5	8	13	21	34	...

Observación 20.5.6.— Alternativamente, pudiésemos haber codificado cada subconjunto como una palabra de n bits donde 1 representa que el número esté en el subconjunto y 0 que no esté. Por ejemplo,

$$\emptyset \rightleftharpoons 0\dots0\dots0,$$
$$\{1, 3, n-3, n\} \rightleftharpoons 1010\dots0\dots01001.$$

De esta manera, por el principio de la biyección, el número de subconjuntos de $\{1, 2, \dots, n\}$ que no contienen números consecutivos coincide con el número de palabras de n bits que no contienen unos consecutivos.

Así, por ejemplo, designando a_n para representar dicho número de palabras, la discusión y distinción de casos, razonando hacia atrás, en el apartado I hubiese sido que hay dos, según la palabra termine o no en 0:

0. si la palabra termina en un bit con valor 0, da igual el valor del bit anterior, habiendo a_{n-1} palabras de $n-1$ bits que no contienen unos consecutivos;
1. si la palabra termina en un bit con valor 1, el bit anterior debe valer 0, habiendo a_{n-2} palabras de $n-2$ bits que no contienen unos consecutivos.

[35] *Vid*. https://oeis.org/A000045.

Observación 20.5.7.— Una vez obtenido el problema de valores iniciales de ecuaciones en diferencias y demostrado que tiene solución única, pudiésemos haberlo solucionado por cualquier otro método estudiado o conocido, sin olvidar que en algunos casos, como por ejemplo, si lo hubiésemos hecho mediante expansión, deberíamos demostrar el resultado seguramente mediante inducción. En nuestra sugerencia de respuesta no hace falta, pues el resultado es consecuencia de la aplicación directa de teoremas (y no de una intuición).

Ejemplo 739

Un robot puede dar pasos de uno o dos metros. Calculemos el número de formas en que el robot puede recorrer n metros.

[EFE 29.1.2025:13] (tipo test), [SEL 12:3]. *Cfr.* Johnsonbaugh [158]: ejemplo 4.4.5 (págs. 206–207).

Resolución.—

1. *Propuesta de una ecuación en diferencias (ED) o más.*

   0. *Discusión previa.*

      Sea a_n el número de formas en que el robot camina n metros.

      Como el robot pueda dar pasos de uno o dos metros, puede haber llegado desde un metro atrás o desde dos metros atrás.

      Si ha llegado desde un metro atrás, entonces, como hay $n-1$ metros desde el origen hasta ese punto, el robot puede haber caminado esta distancia de a_{n-1} formas.

      Por otra parte, y similarmente, si ha llegado desde dos metros atrás, entonces, como hay $n-2$ metros desde el origen hasta ese punto, el robot puede haber caminado esta distancia de a_{n-2} formas.

      Esto ha sido un razonamiento regresivo («hacia atrás»).

      Alternativamente, pudiésemos haber hecho un razonamiento progresivo («hacia adelante»). Veamos.

      Supongamos que el robot está situado en el origen.

      Ahora, puede empezar a caminar dando un paso de un metro o uno de dos metros.

      Si empieza dando un paso de un metro, el resto de la caminata, una distancia de $n-1$ metros, puede completarla de a_{n-1} formas.

      De manera similar, si empieza dando un paso de dos metros, el resto de la caminata, una distancia de $n-2$ metros, puede completarla de a_{n-2} formas.

Calculemos, a continuación, el número pedido mediando el principio de la adición.

1. *Formalización del principio de la adición.*

   Para poder aplicar el principio de la adición debemos definir sucesos incompatibles dos a dos. Estos sucesos son:

$$S_0 \leftrightharpoons \text{recorrer exactamente } n-1 \text{ metros;}$$
$$S_1 \leftrightharpoons \text{recorrer exactamente } n-2 \text{ metros;}$$

   que son incompatibles, puesto que se trata de recorridos con longitudes distintas.

2. *De las formas de suceder los sucesos.*

   Recordemos, hemos llamado a_n al número de formas en que el robot camina n metros.

3. *Aplicación del principio de la adición.*

   Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_0 \cup S_1$. Como hemos dicho ya, son sucesos incompatibles —ya que se trata de recorridos con longitudes distintas—, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

$$\#(S_0 \cup S_1) = \#S_0 + \#S_1,$$

   que en términos de a_n es

$$a_n = a_{n-1} + a_{n-2},$$

   en definitiva,

$$a_n - a_{n-1} - a_{n-2} = 0. \qquad (20.22)$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Los valores iniciales son:

- $a_1 = 1$ (el robot recorre un metro solo de una forma, dando un paso de un metro);
- $a_2 = 2$ (el robot recorre dos metros de dos formas, bien dando dos pasos de un metro, bien dando un paso de dos metros.

El problema de valores iniciales de ecuaciones en diferencias es

$$a_n - a_{n-1} - a_{n-2} = 0 \qquad (3 \leq n),$$
$$a_1 = 1,$$
$$a_2 = 2.$$

III. *Demostración de que dicho PVI tiene solución única.*

Se trata de una ecuación en diferencias de orden 2, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, *tiene una única solución*. En nuestro caso, $k = 2$, esto es, el orden de (20.22) es dos y tenemos dos valores iniciales consecutivos.

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es

$$r^2 - r - 1,$$

por lo que tal ED tiene dos raices características simples, esto es, ambas con multiplicidad uno, y distintas:

$$r_0 = \frac{1-\sqrt{5}}{2},$$
$$r_1 = \frac{1+\sqrt{5}}{2}.$$

V. *Obtención de las soluciones de las ED concernientes.*

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De acuerdo con el teorema 20.12 (pág. 1314 de esta edición) (teorema UNO), cualquier sucesión $\{a_n\}$ que satisfaga (20.22) es de la forma

$$a_n = \rho_0 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n + \rho_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n,$$

para determinados números reales ρ_0 y ρ_1.

Por ello,

$$a_n = \rho_0 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n + \rho_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n \qquad (\rho_0, \rho_1 \in \mathbb{R})$$

es la solución general de (20.22), lo cual significa que existe un número infinito no numerable de sucesiones $\{a_n\}$ que son soluciones particulares de (20.22), cada una de ellas determinada por dos valores reales concretos de ρ_0 y ρ_1.

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo los dos valores iniciales consecutivos en la solución general de (20.22), obtenemos el sistema de dos ecuaciones lineales con dos incógnitas ρ_0 y ρ_1,

$$(a_1 =)1 = \rho_0 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^1 + \rho_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^1,$$
$$(a_2 =)2 = \rho_0 \cdot \left(\frac{1-\sqrt{5}}{2}\right)^2 + \rho_1 \cdot \left(\frac{1+\sqrt{5}}{2}\right)^2,$$

cuya solución es

$$\rho_0 = \frac{\sqrt{5}-1}{2\sqrt{5}},$$
$$\rho_1 = \frac{\sqrt{5}+1}{2\sqrt{5}},$$

esto es, una expresión explícita para $\{a_n\}$ es

$$a_n = \frac{\sqrt{5}-1}{2\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n + \frac{\sqrt{5}+1}{2\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n. \qquad \blacksquare$$

Observación 20.5.8.— Esta sucesión está relacionada con la de los números de FIBONACCI[36] que se define tradicionalmente como

$$F_n = F_{n-1} + F_{n-2} \qquad (n \in \mathbb{Z}^+),$$
$$F_0 = 0,$$
$$F_1 = 1.$$

Recordemos que F_n está catalogada como la sucesión A000045 en la OEIS[37].

Y a_n y F_n están relacionadas porque se satisface

$$a_n = F_{n+1} \qquad (n \in \mathbb{Z}^+),$$

que, por otra parte, es expresable equivalentemente como

$$a_n = \frac{F_n + L_n}{2} \qquad (n \in \mathbb{Z}^+),$$

donde L_n es la sucesión de LUCAS catalogada como la sucesión A000032 en la OEIS[38].

[36] *Vid.* https://es.wikipedia.org/wiki/Sucesión_de_Fibonacci.
[37] *Vid.* https://oeis.org/A000045.
[38] *Vid.* https://oeis.org/A000032.

Ejemplo 740

(*Mini-Tetris, I*). Consideremos un tablero rectangular de $2 \times n$ dividido en $2n$ cuadrados. Calculemos el número de maneras de cubrir exactamente, esto es, por completo y sin superposiciones, este tablero, con piezas rectangulares (dominós) 1×2, estando permitido girar las piezas en ángulos que sean múltiplos de un ángulo recto.

[SEL 12:4]. *Cfr.* Johnsonbaugh [158]: ejercicio 7 (*Self-Test*) (pág. 371).

Resolución.— Esta cuestión es equivalente a la estudiada en el ejemplo 739 (pág. 1341 de esta edición).

1. *Propuesta de una ecuación en diferencias (ED) o más.*

   0. *Discusión previa.*

      Entenderemos por embaldosar, llenar completamente, sin solapamientos, pudiendo las piezas rotar ángulos que sean múltiplos de un ángulo recto.

      Tenemos, pues, que embaldosar un rectángulo $2 \times n$ con piezas 1×2.

      Comenzamos,

      - bien por una pieza 1×2 girada 90°, quedando por embaldosar un rectángulo $2 \times (n-1)$,
      - bien por dos piezas 1×2, quedando por embaldosar un rectángulo $2 \times (n-2)$.

      Calculemos, a continuación, el número pedido mediando el principio de la adición.

   1. *Formalización del principio de la adición.*

      Para poder aplicar el principio de la adición debemos definir sucesos incompatibles dos a dos. Estos sucesos son:

      $$S_0 \leftrightharpoons \text{embaldosar un rectángulo } 2 \times n \text{ comenzando por una pieza } 1 \times 2 \text{ girada } 90^\circ;$$
      $$S_1 \leftrightharpoons \text{embaldosar un rectángulo } 2 \times n \text{ comenzando por dos piezas } 1 \times 2;$$

      que son incompatibles, puesto que se trata de embaldosados distintos.

   2. *De las formas de suceder los sucesos.*

Llamamos $a_n \leftrightharpoons$ número de formas de embaldosar un rectángulo $2 \times n$ en las condiciones dadas en el enunciado.

2. *Aplicación del principio de la adición*.

Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_0 \cup S_1$. Como hemos dicho ya, son sucesos incompatibles —ya que se trata de embaldosados distintos—, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

$$\#(S_0 \cup S_1) = \#S_0 + \#S_1,$$

que en términos de a_n es

$$a_n = a_{n-1} + a_{n-2},$$

en definitiva,

$$a_n - a_{n-1} - a_{n-2} = 0. \tag{20.23}$$

II. *Propuesta de un problema de valores iniciales (PVI)*.

Exploramos posibles valores iniciales:

$a_1 = 1$ (una pieza 1×2 girada $90°$: ▭);

$a_2 = 3$ (configuraciones: ⊟ y ◫);

Observamos, pues, que la sucesión que buscamos tiene como definición implícita *el problema de valores iniciales de ecuaciones en diferencias*

$$a_n - a_{n-1} - a_{n-2} = 0, \text{ para } n > 1,$$
$$a_1 = 1, \tag{20.24}$$
$$a_2 = 2. \tag{20.25}$$

En definitiva, que esta cuestión es equivalente a la estudiada en el ejemplo 739 (pág. 1341 de esta edición). En efecto, la longitud n de la caminata es equivalente a la longitud n del tablero, cada paso de un metro es equivalente a situar una pieza 1×2 girada $90°$ ⊟, y cada paso de dos metros es equivalente a situar dos dos piezas 1×2 ◫.

A dicho ejemplo remitimos para ver la resolución de los apartados III, IV, V y VI.

Solución.— El número de maneras de llenar completamente y sin solapamientos un rectángulo de dimensiones $2 \times n$ con piezas rectangulares 1×2, pudiendo éstas rotar ángulos que sean múltiplos

de 90°, viene dado por a_n que, en función de los números de FIBONACCI, es

$$a_n = F_{n+1} \qquad (n > 0).$$ 

Ejemplo 741

Un dispositivo emite constantemente señales sonoras de tres tipos (bip, chof-chof y toc-toc) sin superposiciones. Una señal bip dura un segundo, una señal chof-chof, dos segundos y una señal toc-toc, también dos segundos. En n segundos, ¿de cuántas formas diferentes puede sonar dicho dispositivo?, en otras palabras, ¿de cuántas formas distintas puede el mencionado dispositivo llenar completamente y sin superposiciones un tiempo de n segundos con dichas señales sonoras bip, chof-chof y toc-toc?

[EFE 28.6.2023:9].

Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más.*

0. *Discusión previa.*

Tenemos que llenar un tiempo de n segundos con señales sonoras bip, chof-chof y toc-toc, sin superposiciones.

Comenzamos tal relleno,

- bien por una señal bip, quedando por emitir señales en los siguientes $n-1$ segundos,
- bien por una señal chof-chof, quedando por emitir señales en los siguientes $n-2$ segundos,
- bien por una señal toc-toc, quedando por emitir señales en los siguientes $n-2$ segundos.

Calculemos el número pedido mediando el principio de la adición (*cfr. supra* § 19.1.0 [pág. 1136 de esta edición]).

1. *Formalización del principio de la adición.*

Definimos tres sucesos incompatibles dos a dos:

$S_0 \leftrightharpoons$ emitir señales sonoras durante n segundos comenzando por una señal bip;
$S_1 \leftrightharpoons$ emitir señales sonoras durante n segundos comenzando por una señal chof-chof;
$S_2 \leftrightharpoons$ emitir señales sonoras durante n segundos comenzando por una señal toc-toc;

que son incompatibles dos a dos, puesto que las tres señales sonoras son distintas.

2. *De las formas de suceder los sucesos*.

   Llamamos $a_n \leftrightharpoons$ número de formas de emitir señales sonoras durante n segundos.

3. *Aplicación del principio de la adición*.

   Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_0 \cup S_1 \cup S_2$. Como hemos dicho ya, son sucesos incompatibles dos a dos, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

$$\#(S_0 \cup S_1 \cup S_2) = \#S_0 + \#S_1 + \#S_2,$$

   que en términos de a_n es

$$a_n = a_{n-1} + a_{n-2} + a_{n-2},$$

   en definitiva,

$$a_n - a_{n-1} - 2a_{n-2} = 0. \tag{20.26}$$

II. *Propuesta de un problema de valores iniciales (PVI)*.

Exploramos algunos primeros valores iniciales (descartamos $n = 0$ por significar llenar un tiempo de cero segundos y ser esto independiente de las tres señales):

- $a_1 = 1$ (una señal sonora bip);
- $a_2 = 3$ (configuraciones: bip, bip; chof-chof; toc-toc);
- $a_3 = 5$ (configuraciones: bip, bip, bip; bip, chof-chof; bip, toc-toc; chof-chof, bip; toc-toc, bip).

Observamos, pues, que la sucesión que buscamos tiene como definición implícita *el problema de valores iniciales de ecuaciones en diferencias* (PVI)

$$a_n - a_{n-1} - 2a_{n-2} = 0 \quad n \geq 2,$$

$$a_1 = 1, \tag{20.27}$$

$$a_2 = 3. \tag{20.28}$$

III. *Demostración de que dicho PVI tiene solución única*.

Se trata de una ecuación en diferencias de orden 2, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, *tiene una única solución*. En nuestro caso, $k = 2$ —el orden de (20.26) es 2 y tenemos dos valores iniciales consecutivos—.

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es $x^2 - x - 2$, siendo $r_0 = -1$ y $r_1 = 2$ las dos raices características simples, esto es, ambas con multiplicidad uno, y distintas.

V. *Obtención de las soluciones de las ED concernientes.*

0. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

   Por el teorema 20.12 (pág. 1314 de esta edición) (teorema UNO), *la solución general* es

$$a_n = c_{r_0}(-1)^n + c_{r_1}2^n \qquad (c_{r_0}, c_{r_1} \in \mathbb{R}). \tag{20.29}$$

1. *Obtención de una solución particular de la completa* (Paso III de ARED5).

   No procede (la ED es homogénea).

2. *Obtención de la solución general de la completa* (Paso IV de ARED5).

   No procede (la ED es homogénea).

VI. *Obtención de la solución del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo los dos valores iniciales consecutivos (20.33) y (20.34) en (20.29) tenemos el sistema de dos ecuaciones con dos incógnitas

$$a_1 = 1 = c_{r_0}(-1)^1 + c_{r_1}2^1,$$
$$a_2 = 3 = c_{r_0}(-1)^2 + c_{r_1}2^2,$$

de donde:

$$c_{r_0} = \frac{1}{3}, \tag{20.30}$$
$$c_{r_1} = \frac{2}{3}. \tag{20.31}$$

Sustituyendo (20.30) y (20.31) en (20.29), obtenemos la sucesión buscada

$$a_n = \frac{1}{3}(-1)^n + \frac{2}{3}2^n.$$

Solución.— El número de formas de llenar completamente y sin superposiciones un tiempo de n segundos con señales sonoras bip, chof-chof y toc-toc, viene dado por

$$a_n = \frac{1}{3}\left((-1)^n + 2^{n+1}\right) \qquad (n \geq 1).$$ ■

Observación 20.5.9.— Para todo n entero positivo,

$$a_n = J_{n+1},$$

donde $\{J_n\}$ es la sucesión de JACOBSTHAL, catalogada como la sucesión A001045 en la OEIS[39], donde encontramos diversas fórmulas e interpretaciones.

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
a_n	—	1	3	5	11	21	43	85	171	341	...
J_n	0	1	1	3	5	11	21	43	85	171	...

Observación 20.5.10.— El enésimo número de JACOBSTHAL, J_n, se expresa, a la vez que se define, como el problema de valores iniciales

$$\begin{aligned} J_n &= J_{n-1} + 2J_{n-2} \quad (1 < n), \\ F_0 &= 0, \\ F_1 &= 1. \end{aligned}$$

Observación 20.5.11.— *Vid.* la observación 20.5.7 (pág. 1341 de esta edición).

Ejemplo 742

(*Mini-Tetris, II*). Consideremos un tablero rectangular de $2 \times n$ dividido en $2n$ cuadrados. Calculemos el número de maneras de cubrir exactamente, esto es, por completo y sin superposiciones, este tablero, con piezas rectangulares (dominós) 1×2 y cuadradas 2×2, estando permitido girar las piezas en ángulos que sean múltiplos de un ángulo recto.

[EFO 4.6.2021:10], [EFO 24.5.2023:9].

Resolución.— Esta cuestión es equivalente a la estudiada en el ejemplo 741 (pág. 1347 de esta edición).

1. *Propuesta de una ecuación en diferencias (ED) o más.*

   0. *Discusión previa.*

   Entenderemos por embaldosar, llenar completamente, sin solapamientos, pudiendo las piezas rotar ángulos que sean múltiplos de un ángulo recto.

[39] *Vid.* https://oeis.org/A001045.

Tenemos, pues, que embaldosar un rectángulo $2 \times n$ con piezas 1×2 y piezas 2×2.

Comenzamos,

- bien por una pieza 1×2 girada 90°, quedando por embaldosar un rectángulo $2 \times (n-1)$,
- bien por dos piezas 1×2, quedando por embaldosar un rectángulo $2 \times (n-2)$,
- bien por una pieza 2×2, quedando por embaldosar un rectángulo $2 \times (n-2)$.

Calculemos, a continuación, el número pedido mediando el principio de la adición.

1. *Formalización del principio de la adición.*

   Para poder aplicar el principio de la adición debemos definir sucesos incompatibles dos a dos. Estos sucesos son:

   $$\begin{aligned} S_0 &\leftrightharpoons \text{embaldosar un rectángulo } 2 \times n \text{ comenzando por una pieza } 1 \times 2 \text{ girada } 90^\circ; \\ S_1 &\leftrightharpoons \text{embaldosar un rectángulo } 2 \times n \text{ comenzando por dos piezas } 1 \times 2; \\ S_2 &\leftrightharpoons \text{embaldosar un rectángulo } 2 \times n \text{ comenzando por una pieza } 2 \times 2; \end{aligned}$$

   que son incompatibles dos a dos, puesto que se trata de embaldosados distintos.

2. *De las formas de suceder los sucesos.*

   Llamamos $a_n \leftrightharpoons$ número de formas de embaldosar un rectángulo $2 \times n$ en las condiciones del enunciado.

2. *Aplicación del principio de la adición.*

   Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_0 \cup S_1 \cup S_2$. Como hemos dicho ya, son sucesos incompatibles dos a dos —ya que se trata de embaldosados distintos—, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

   $$\#(S_0 \cup S_1 \cup S_2) = \#S_0 + \#S_1 + \#S_2,$$

   que en términos de a_n es

   $$a_n = a_{n-1} + a_{n-2} + a_{n-2},$$

en definitiva,

$$a_n - a_{n-1} - 2a_{n-2} = 0. \tag{20.32}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Exploramos posibles valores iniciales:

$a_1 = 1$ (una pieza 1×2 girada $90°$:);

$a_2 = 3$ (configuraciones: , y);

$a_3 = 5$ (configuraciones: , , , y).

Observamos, pues, que la sucesión que buscamos tiene como definición implícita *el problema de valores iniciales de ecuaciones en diferencias*

$$a_n - a_{n-1} - 2a_{n-2} = 0, \text{ para } n > 2,$$

$$a_1 = 1, \tag{20.33}$$

$$a_2 = 3. \tag{20.34}$$

En definitiva, esta cuestión es equivalente a la estudiada en el ejemplo 741 (pág. 1347 de esta edición). A él remitimos para ver la resolución de los apartados III, IV, V y VI.

Solución.— El número de maneras de llenar completamente y sin solapamientos un rectángulo de dimensiones $2 \times n$ con piezas rectangulares 1×2 y cuadradas 2×2 pudiendo las piezas rotar ángulos que sean múltiplos de $90°$, viene dado por

$$a_n = \frac{1}{3}\left((-1)^n + 2^{n+1}\right) \qquad (n > 0).$$ ■

Observación 20.5.12.— Como ya dijimos en la observación 20.5.9 (pág. 1350 de esta edición), para todo n entero positivo, $a_n = J_{n+1}$, donde $\{J_n\}$ es la sucesión de Jacobsthal. En la OEIS[40] encontramos diversas fórmulas e interpretaciones, por ejemplo, referidas a esta cuestión, J_n es el «número de formas de embaldosar un rectángulo $2 \times (n-1)$ con balsosas 1×2 y cuadradas 2×2» y también el «número de formas de embaldosar un rectángulo $3 \times (n-1)$ con baldosas cuadradas 1×1 y 2×2».

[40] *Vid.* https://oeis.org/A001045.

Ejemplo 743

Tenemos n monedas del mismo valor y que en cada compra, compramos o bien un objeto de tipo A, que cuesta una moneda, o bien uno de tipo B, que cuesta dos monedas o bien uno de tipo C, que también cuesta dos monedas. ¿De cuántas formas es posible gastar las n monedas? Tenemos en cuenta el orden, por ejemplo, para tres monedas hay cinco formas:

AAA (tres compras, comprando un objeto A en cada una),
AB (dos compras, comprando un objeto A en la primera y un objeto B en la segunda),
BA (dos compras, comprando un objeto B en la primera y un objeto A en la segunda),
AC (dos compras, comprando un objeto A en la primera y un objeto C en la segunda),
CA (dos compras, comprando un objeto C en la primera y un objeto A en la segunda).

Resolución.— Esta cuestión es equivalente a las estudiadas en el ejemplo 741 (pág. 1347 de esta edición) y en el ejemplo 742 (pág. 1350 de esta edición).

I. *Propuesta de una ecuación en diferencias (ED) o más.*

Sea a_n el número de formas en las que se pueden gastar las n monedas.

En la primera compra, puede ocurrir:

- bien que compremos un objeto de tipo A, con lo que gastamos una moneda, por lo que nos quedan $n-1$ monedas, que podrán gastarse de a_{n-1} formas,
- bien que compremos un objeto de tipo B o uno de tipo C, con lo que, en cada caso, gastamos dos monedas, por lo que nos quedan $n-2$ monedas, que podrán gastarse de a_{n-2} formas.

Como todas estos sucesos son incompatibles dos a dos, entonces, por el principio de la adición,

$$a_n = a_{n-1} + 2a_{n-2}. \tag{20.35}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Para encontrar la solución a la cuestión, necesitamos dos valores iniciales consecutivos —*cfr. supra* teorema 20.4 (pág. 1302 de esta edición) (teorema CERO)—, que son:

- $a_1 = 1$ (se gasta de una forma, en una compra, comprando un objeto de tipo A);
- $a_2 = 3$ (se gastan de tres formas: I, en dos compras, comprando en cada una un objeto de tipo A; o bien, II, en una sola compra de un objeto de tipo B, o bien, III, en una sola compra de un objeto de tipo C; abreviadamente: AA, B, C).

El problema de valores iniciales de ecuaciones en diferencias es

$$a_n - a_{n-1} - 2a_{n-2} = 0 \qquad (2 \leq n),$$
$$a_1 = 1,$$
$$a_2 = 3.$$

En definitiva, esta cuestión es equivalente a la que estudiamos en el ejemplo 741 (pág. 1347 de esta edición). A él remitimos para ver la resolución detallada de los apartados III, IV, V y VI.

Solución.— El número de formas posibles (sucesos elementales) en que es posible gastar las n monedas es, viene dado por

$$a_n = \frac{1}{3}\left((-1)^n + 2^{n+1}\right) \qquad (n \geq 1). \qquad \blacksquare$$

Observación 20.5.13.— Como ya dijimos en la observación 20.5.9 (pág. 1350 de esta edición), para todo n entero positivo, $a_n = J_{n+1}$, donde $\{J_n\}$ es la sucesión de Jacobsthal.

Actividad 20.7

En el ejemplo anterior, el razonamiento que hemos hecho para formalizar la ecuación en diferencias ha sido «hacia adelante»; es muy recomendable que pensemos también en un razonamiento «hacia atrás», esto es, partiendo de que ya se han gastado las n monedas.

Ejemplo 744

¿Cuántas banderas de n franjas horizontales hay si cada franja puede colorearse con un único color de tres disponibles y no pueden ser del mismo color ni dos franjas contiguas ni las franjas primera y última? (Puede ser una buena idea comprobar el resultado para banderas de hasta cuatro franjas).

[EFO 17.1.2022:9]. *Cfr.* García, Hernández y Nevot [150]: problema resuelto 6.1 (pág. 276).

Resolución.—

1. *Propuesta de una ecuación en diferencias (ED) o más.*

Si bien la cuestión no es equivalente, la ecuación en diferencias que formaliza la presente es la misma que las estudiadas en los ejemplos 741 (pág. 1347 de esta edición), 742 (pág. 1350 de esta edición) y 746 (pág. 1359 de esta edición):

- una bandera de $n-1$ franjas se extiende a una de n franjas coloreando la franja n con el color no utilizado en las franjas 1 y $n-1$; se obtienen a_{n-1} banderas;

- una bandera de $n-2$ franjas se extiende a una de n franjas, repitiendo en la $n-1$ el color de la 1, digamos x, y coloreando la n con cualquiera de los otros dos colores, digamos y y z:
  - con el color y se obtienen a_{n-2} banderas, y
  - con el color z se obtienen a_{n-2} banderas;
- cualquier bandera se obtiene de lo anterior: si los colores de la 1 y de la $n-1$ son iguales, procede del segundo caso, y si son distintos, procede del primer caso.

Subyace el *principio de la adición*: estos casos (sucesos, en realidad) se excluyen mutuamente (son incompatibles, ya que cada bandera sólo puede ser de un tipo) y su unión es el suceso colorear todas las banderas de n franjas horizontales en las condiciones del enunciado, entonces, por el principio de la adición, dicho suceso unión sucede de $a_n = a_{n-1} + a_{n-2} + a_{n-2}$ formas distintas, en definitiva,

$$a_n - a_{n-1} - 2a_{n-2} = 0. \tag{20.36}$$

II. *Propuesta de un problema de valores iniciales (PVI)*.

Supongamos que los colores son blanco (B), rojo (R) y verde (V). Los valores iniciales:

- $a_1 = 3$, las banderas de una franja B, R y V;
- $a_2 = 6$, las banderas de dos franjas BR, BV, RV, RB, VB, VR;
- $a_3 = 6$, las banderas de tres franjas BRV, BVR, RBV, RVB, VBR, VRB.
- $a_4 = 18$, las banderas de cuatro franjas BRVR, BRBR, BRBV, BVRV, BVBV, BVBR, RBVB, RBRB, RBRV, RVBV, RVRV, RVRB, VBRB, VBVB, VBVR, VRBR, VRVR, VRVB.

Si bien pudiese parecer que se satisface la ecuación (20.36) para $n \geq 3$, no es así, pues $a_3 = 6 \neq 6 + 2 * 3 = a_2 + 2a_1$. Lo cierto es que dicha ecuación se satisface para $n \geq 4$.

Observamos, pues, que la sucesión que buscamos tiene como definición implícita *el problema de valores iniciales de ecuaciones en diferencias* (PVI)

$$a_n - a_{n-1} - 2a_{n-2} = 0 \quad n \geq 4,$$

$$a_2 = 6, \tag{20.37}$$

$$a_3 = 6. \tag{20.38}$$

III. *Demostración de que dicho PVI tiene solución única*.

Se trata de una ecuación en diferencias de orden 2, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y

k condiciones iniciales consecutivas, *tiene una única solución*. En nuestro caso, $k = 2$ —el orden de (20.36) es 2 y tenemos dos valores iniciales consecutivos—.

IV. *Cálculo de las raíces características pertinentes*.

Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es $x^2 - x - 2$, siendo $r_0 = -1$ y $r_1 = 2$ las dos raices características simples, esto es, ambas con multiplicidad 1, y distintas.

V. *Obtención de las soluciones de las ED concernientes*.

0. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De lo anterior que por un teorema conocido —teorema 20.12 (pág. 1314 de esta edición) (teorema UNO) o teorema 20.15 (pág. 1327 de esta edición) (teorema CUATRO)— *la solución general* es:

$$a_n = c_{r_0}(-1)^n + c_{r_1}2^n \qquad (c_{r_0}, c_{r_1} \in \mathbb{R}). \tag{20.39}$$

1. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

2. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo los dos valores iniciales consecutivos (20.37) y (20.38) en (20.29) tenemos el sistema de dos ecuaciones con dos incógnitas

$$(a_2 =)6 = c_{r_0}(-1)^2 + c_{r_1}2^2,$$
$$(a_3) = 6 = c_{r_0}(-1)^3 + c_{r_1}2^3,$$

de donde:

$$c_{r_0} = 2, \tag{20.40}$$
$$c_{r_1} = 1. \tag{20.41}$$

Sustituyendo (20.40) y (20.41) en (20.39), obtenemos $a_n = 2 \cdot (-1)^n + 1 \cdot 2^n$.

Solución.— El número de banderas de n franjas horizontales, si cada franja puede colorearse con un único color de tres disponibles y no pueden ser del mismo color ni dos franjas contiguas ni las

franjas primera y última, viene dado por

$$a_n = 2(-1)^n + 2^n \qquad (n \geq 2).$$ 

Observación 20.5.14.— Para $n \geq 2$, a_n está catalogada como la sucesión A092297 en la OEIS[41], donde encontramos diversas fórmulas e interpretaciones.

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
a_n	—	3	6	6	18	30	66	126	258	510	...

Ejemplo 745

Una granja de cómputo dispone de tres tipos de computadores. Alquilar un minuto de cómputo de un computador del primer tipo cuesta un euro; alquilarlo de un computador del segundo o tercer tipo cuesta dos euros. ¿De cuántas formas pueden gastarse n euros en alquilar minutos de cómputo en esta granja?

[EFE 7.7.2021:10], [SEP 12.5.2022:10], [EFE 22.6.2022:10], [EFE 29.1.2025:15] (tipo test). *Cfr.* García, Hernández y Nevot [150]: problema resuelto 6.10 (pág. 265).

Resolución.— Esta cuestión es equivalente a la estudiada en los ejemplos 741 (pág. 1347 de esta edición), 742 (pág. 1350 de esta edición) y 746 (pág. 1359 de esta edición) y tiene la misma ecuación en diferencias (aunque no los mismos valores iniciales) que la estudiada en el ejemplo 744 (pág. 1354 de esta edición).

En efecto.

1. *Propuesta de una ecuación en diferencias (ED) o más.*

   Designemos a_n para representar el número de formas buscado. Para construir una ecuación en diferencias para a_n, razonemos hacia atrás, observando el último alquiler realizado. Pueden suceder tres casos:

   0. que el último alquiler haya sido un minuto de cómputo de un computador del primer tipo, entonces los $n-1$ euros restantes se han gastado de a_{n-1} formas;

   1. que el último alquiler haya sido un minuto de cómputo de un computador del segundo tipo, entonces los $n-2$ euros restantes se han gastado de a_{n-2} formas;

   2. que el último alquiler haya sido un minuto de cómputo de un computador del tercer tipo, entonces los $n-2$ euros restantes se han gastado de a_{n-2} formas.

[41] *Vid*. https://oeis.org/A092297.

Ya intuimos la equivalencia con el ejemplo mencionado; como allí, subyace el *principio de la adición*: estos casos (sucesos, en realidad) se excluyen mutuamente (son incompatibles, ya que cada computador sólo puede ser de un tipo) y su unión es el suceso gastar los n euros en alquilar minutos de cómputo en esa granja, entonces, por el principio de la adición, dicho suceso unión sucede de $a_n = a_{n-1} + a_{n-2} + a_{n-2}$ formas distintas, en definitiva,

$$a_n - a_{n-1} - 2a_{n-2} = 0. \qquad (20.42)$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Por ser esta ecuación en diferencias lineal homogénea de coeficientes constantes y orden dos, del teorema 20.4 (pág. 1302 de esta edición) (teorema CERO) se sigue que basta con un valor inicial para conformar un problema de valores iniciales de ecuaciones en diferencias que tenga una solución única.

Exploramos posibles valores iniciales:

$a_1 = 1$ (sólo es posible alquilar un minuto de cómputo en un computador del primer tipo);

$a_2 = 3$ (pueden, bien alquilarse dos minutos de cómputo de dos computadores del primer tipo —uno en cada uno—, bien dos minutos de cómputo de un computador del segundo tipo, bien dos minutos de cómputo de un computador del tercer tipo).

Observamos, pues, que la sucesión que buscamos tiene como definición implícita *el problema de valores iniciales de ecuaciones en diferencias*

$$\begin{aligned} a_n - a_{n-1} - 2a_{n-2} &= 0 \qquad (n > 2) \\ a_1 &= 1 \\ a_2 &= 3 \end{aligned}$$

En definitiva, esta cuestión es equivalente a la estudiada en el ejemplo 741 (pág. 1347 de esta edición). A él remitimos para estudiar la resolución de los apartados III, IV, V y VI.

Solución.— El número de formas en que pueden gastarse n euros en alquilar minutos de cómputo en esta granja viene dado por

$$a_n = \frac{1}{3}\left((-1)^n + 2^{n+1}\right) \qquad (n > 0).$$ ■

Observación 20.5.15.— Como ya dijimos en la observación 20.5.9 (pág. 1350 de esta edición), para todo n entero positivo, $a_n = J_{n+1}$, donde $\{J_n\}$ es la sucesión de Jacobsthal.

Ejemplo 746

Queremos transportar n objetos de tres tamaños distintos A, B, y C, desde el sitio P al sitio Q. De una vez, es posible que transportemos, o bien un objeto de tamaño A, o bien uno de tamaño B o bien dos de tamaño C. La cuestión es averiguar de cuántas formas pueden transportarse los n objetos desde el sitio P al sitio Q.

[EFE 29.1.2025:14] (tipo test).

Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más.*

Sea a_n el número de formas en las que se pueden transportar los n objetos.

En el primer transporte, puede ocurrir:

- bien que transportemos un objeto de tamaño A o uno de tamaño B, con lo que quedan, en cada caso, $n-1$ objetos por transportar, que podremos transportar de a_{n-1} formas,
- bien que transportemos dos objetos de tamaño C, con lo que quedan $n-2$ objetos por transportar, que podremos transportarse de a_{n-2} formas.

Como «transportar exactamente $n-1$ objetos de un lugar a otro» y «transportar exactamente $n-2$ objetos de un lugar a otro» son sucesos incompatibles dos a dos, entonces, por el principio de la adición [¡esto requiere justificación! ✍],

$$a_n = 2a_{n-1} + a_{n-2}. \qquad (20.43)$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Como (20.43) es una ecuación en diferencias de orden dos, según el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), teniendo dos valores iniciales consecutivos, tenemos una solución particular.

Exploremos algunos valores iniciales:

- $a_1 = 1$, una forma, a saber, sólo un transporte, transportando el único objeto que hay;
- $a_2 = 2$, dos formas, que son:
  - un sólo transporte en el caso de haber dos objetos de tamaño C, o bien,
  - dos transportes en el resto de casos, esto es, si hay sólo un objeto de tamaño C o ninguno;
- $a_3 = 5$, ya que:

- si hay exactamente cero o un objetos de tamaño C, una forma (necesariamente en tres transportes [un objeto cada vez]);
- si hay exactamente dos objetos de tamaño C, dos formas (en dos transportes [dos objetos en un transporte y un objeto en otro transporte] o en tres [un objeto cada vez]);
- si hay exactamente tres objetos de tamaño C, dos formas (en dos transportes [dos objetos en un transporte y un objeto en otro transporte] o en tres [un objeto cada vez]).

El problema de valores iniciales es

$$\begin{aligned} a_n - 2a_{n-1} - a_{n-2} &= 0 \qquad (3 \leq n), \\ a_1 &= 1, \\ a_2 &= 2. \end{aligned}$$

III. *Demostración de que dicho PVI tiene solución única*.

Se trata de una ecuación en diferencias de orden dos, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, *tiene una única solución*. En nuestro caso, $k = 2$ —el orden de (20.43) es dos y tenemos dos valores iniciales consecutivos—.

IV. *Cálculo de las raíces características pertinentes*.

Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es $r^2 - 2r - 1$, siendo $r_0 = 1 - \sqrt{2}$ y $r_1 = 1 + \sqrt{2}$ las dos raices características simples, esto es, ambas con multiplicidad uno, y distintas.

V. *Obtención de las soluciones de las ED concernientes*.

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De acuerdo con el teorema 20.12 (pág. 1314 de esta edición) (teorema UNO), cualquier sucesión $\{a_n\}$ que satisfaga (20.43) es de la forma

$$a_n = \rho_0 \cdot (1 - \sqrt{2})^n + \rho_1 \cdot (1 + \sqrt{2})^n,$$

para determinados números reales ρ_0 y ρ_1.

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo los dos valores iniciales consecutivos en la solución general hallada de (20.43), obtenemos el siguiente sistema de dos ecuaciones lineales con dos incógnitas ρ_0 y ρ_1:

$$(a_1 = 1) = \rho_0 \cdot (1 - \sqrt{2})^1 + \rho_1 \cdot (1 + \sqrt{2})^1,$$
$$(a_2 = 2) = \rho_0 \cdot (1 - \sqrt{2})^2 + \rho_1 \cdot (1 + \sqrt{2})^2,$$

cuya solución es

$$\rho_0 = -\frac{1}{2\sqrt{2}},$$
$$\rho_1 = \frac{1}{2\sqrt{2}},$$

esto es, una expresión explícita para $\{a_n\}$ es

$$a_n = -\frac{1}{2\sqrt{2}} \cdot (1 - \sqrt{2})^n + \frac{1}{2\sqrt{2}} \cdot (1 + \sqrt{2})^n,$$

es decir,

$$a_n = \frac{(1 + \sqrt{2})^n - (1 - \sqrt{2})^n}{2\sqrt{2}}.$$

Solución.— De $\left((1+\sqrt{2})^n - (1-\sqrt{2})^n\right) / \left(2\sqrt{2}\right)$ formas resulta posible transportar n objetos desde P a Q. ■

Actividad 20.8

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Observación 20.5.16.— La sucesión a_n no es otra que la *sucesión de los números de* PELL, $\langle P_n \rangle_{n \geq 0}$ y está catalogada como la sucesión A000129 en la OEIS[42], donde encontramos diversas fórmulas e interpretaciones.

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
P_n	0	1	2	5	12	29	70	169	408	985	...

[42] *Vid*. https://oeis.org/A000129.

Actividad 20.9

En la solución aparece $1+\sqrt{2}$, ¿qué tiene que ver la sucesión de PELL con el número de plata*?

* *Vid. supra Números metálicos, la matemática y el diseño* (pág. 773 de esta edición).

§ 20.5.1 EDLCC no homogéneas

Ejemplo 747

Sea el arenero de un experimento web con una población de bots autorreplicantes malignos tal que no existen factores externos que modifiquen su crecimiento. Supongamos una población inicial de cien bots, que ésta duplica su número en cada generación y que, además, diez nuevos bots se incorporan en cada generación procedentes de la RUD contaminada. Calculemos el número de bots en la generación enésima.

[SEL 13:7a].

Resolución.— Sea b_n el número de bots autorreplicantes malignos en la generación n.

Deducimos del enunciado, que

$$b_n = 2b_{n-1} + 10,$$

la cual es una ecuación en diferencias lineal no homogénea con coeficientes constantes y de grado uno, por lo que según el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), teniendo un valor inicial, tenemos una solución particular; este valor inicial es $b_0 = 100$.

Así, el problema de valores iniciales de ecuaciones en diferencias que nos interesa es

$$b_n - 2b_{n-1} = 10 \qquad (n > 0), \tag{20.44}$$

$$b_0 = 100. \tag{20.45}$$

Pudiésemos, como en tantos ejemplos, seguir el procedimiento sistemático en 5 pasos, si bien procedemos a intentar una demostración por iteración, esto es, por sustitución hacia adelante (SHA):

- *Expansión.*— Iteramos $b_n = 2b_{n-1} + 10$ recorriendo los valores de n, de 0 en adelante:

$$\begin{aligned}
b_0 &= 100,\\
b_1 &= 2b_0 + 10 = 2\cdot 100 + 10 = 2^1\cdot 100 + 2^0\cdot 10,\\
b_2 &= 2b_1 + 10 = 2\cdot(2\cdot 100 + 10) + 10 = 2\cdot 2\cdot 100 + 2\cdot 10 + 10\\
&= 2^2\cdot 100 + 2^1\cdot 10 + 2^0\cdot 10,
\end{aligned}$$

$$\begin{aligned} b_3 &= 2b_2 + 10 = 2 \cdot (2 \cdot 2 \cdot 100 + 2 \cdot 10 + 10) + 10 \\ &= 2 \cdot 2 \cdot 2 \cdot 100 + 2 \cdot 2 \cdot 10 + 2 \cdot 10 + 10 \\ &= 2^3 \cdot 100 + 2^2 \cdot 10 + 2^1 \cdot 10 + 2^0 \cdot 10, \\ &\ \vdots \end{aligned}$$

- *Intuición.*— Tratamos de intuir una expresión general para b_n:

$$\begin{aligned} &\ \vdots \\ b_n &= 2^n \cdot 100 + 2^{n-1} \cdot 10 + 2^{n-2} \cdot 10 + \cdots + 2^1 \cdot 10 + 2^0 \cdot 10 \\ &= 2^n \cdot 100 + (2^{n-1} + 2^{n-2} + \cdots + 2^1 + 2^0) \cdot 10 \\ &= 2^n \cdot 100 + (2^n - 1) \cdot 10 \text{ [suma parcial de una progresión geométrica de razón 2]}^* \\ &= 110 \cdot 2^n - 10. \end{aligned}$$

* La suma parcial de los n primeros términos, desde $a_0 = 2^0$ hasta $a_{n-1} = 2^{n-1}$, con razón $r = 1$, esto es, $S_n = a_0(r^n - 1)/(r - 1) = 2^0(2^n - 1)/(2 - 1) = 2^n - 1$.

- *Demostración.*— Queda demostrar lo intuido, esto es, que $(\forall n \in \mathbb{N})\ (b_n = 110 \cdot 2^n - 10)$; por ejemplo, por inducción débil. Sea $P(n) \leftrightharpoons 110 \cdot 2^n - 10$. Apliquemos inducción débil (*cfr. supra* teorema 16.0 —pág. 805—):

  Caso base (ID$_0$).— $P(0)$ se satisface, ya que $110 - 10 = 100$, que es el valor de b_0.

  Paso inductivo (ID$_0$).— Supongamos $P(k)$, esto es, $110 \cdot 2^k - 10$, y preguntémonos $P(k+1)$, es decir, $110 \cdot 2^{k+1} - 10$; pues bien,

$$\begin{aligned} b_{k+1} &= 2b_k + 10 \\ &= 2 \cdot (110 \cdot 2^k - 10) + 10 \\ &= 110 \cdot 2^{k+1} - 10. \end{aligned}$$

  Conclusión (ID$_0 \wedge$ ID$_1$).— Como se satisfacen el caso base y el paso inductivo, entonces, por el teorema 16.0 (pág. 805 de esta edición), de inducción débil, se tiene lo buscado, a saber, que $(\forall n \in \mathbb{N})\ (110 \cdot 2^n - 10)$. ■

En definitiva, la solución del problema de valores iniciales de ecuaciones en diferencias es

$$b_n = 110 \cdot 2^n - 10.$$

Solución.— El número de bots en la generación enésima es $110 \cdot 2^n - 10$.

Observación 20.5.17.— La solución al ejemplo anterior es

$$\begin{aligned} b_n &= 110 \cdot 2^n - 10 \\ &= 10 \cdot (11 \cdot 2^n - 1) \\ &= 10a_n, \end{aligned}$$

donde a_n es la sucesión catalogada como A086225 en la OEIS[43].

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
a_n	10	21	43	87	175	351	703	1407	2815	5631	...

Ejemplo 748

En $\mathbb{N}$, se define la suma de dos naturales m y n en la forma:

$$\begin{aligned} S(n, 0) &= n, \\ S(n, m) &= S(n, m-1) + 1. \end{aligned}$$

Demostremos que la solución única de este PVI es $S(n, m) = n + m$.

[Cubit 160].

Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más.*

Observemos que n es ajena a la recursión. Así, de una manera más sencilla pero equivalente, denotando $S(n, m)$ por $f(m)$, estamos ante una ecuación en diferencias lineal no homogénea con coeficientes constantes, con función constante en el segundo miembro de la igualdad (la parte no homogénea),

$$f(m) - f(m-1) = 1. \tag{20.46}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Siguiendo con la denotación, tenemos el PVI

$$\begin{aligned} f(m) - f(m-1) &= 1, \\ f(0) &= n. \end{aligned}$$

III. *Demostración de que dicho PVI tiene solución única.*

[43] *Vid.* https://oeis.org/A086225.

Como (20.46) es de orden uno ($|m-(m-1)|=1$) y conocemos un valor inicial, se sigue del teorema 20.4 (pág. 1302 de esta edición) (teorema CERO) que el PVI tiene una única solución.

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada a (20.46) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es $P(x)=x-1$ por lo que 1 es raíz característica simple (multiplicidad uno).

V. *Obtención de las soluciones de las ED concernientes.*

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

Por el teorema 20.14 (pág. 1325 de esta edición) (teorema TRES), la solución general de la homogénea es

$$f^{(h)}(m)=c_1 1^m \qquad (c_1\in\mathbb{R}).$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

$F(n)=1=1\cdot 1^n$, esto es, $b_0=1$ y $s=1$.

Del el teorema 20.17 (pág. 1328 de esta edición) (teorema SEIS), como $s=1$ es raíz de la homogénea asociada con multiplicidad $m_s=1$, se sigue que $n^1 p_0 1^n$, esto es, $f^{(p)}(m)=p_0 m$, en este ejemplo, es una solución particular de la completa.

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

Por el el teorema 20.16 (pág. 1328 de esta edición) (teorema CINCO), es $\{f^{(h)}(m)\}+\{f^{(p)}(m)\}$, esto es,

$$c_1+p_0 m \qquad (c_1,p_0\in\mathbb{R}).$$

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Incorporación de las condiciones iniciales.

Sabemos que $f(0)=n$. Por tanto,

$$(f(0)=)n=c_1+p_0\cdot 0,$$

de donde

$$c_1=n.$$

Sustituyendo en (20.46), obtenemos la solución buscada, $f(m)=n+m$, es decir, $S(n,m)=n+m$. ■

Ejemplo 749

Calculemos el número de saludos que suceden entre n personas si todas se saludan entre sí una, y sólo una, vez (y ninguna persona se saluda a sí misma).

[EFE 28.6.2023:10], [EFO 27.5.2025:9], [EFE 18.6.2025:9], [SEL 13:3]. *Cfr.* GRIMALDI [155]: ejemplo 10.30 (págs. 490–491).

Resolución.—

1. *Propuesta de una ecuación en diferencias (ED) o más.*

Pensemos en una reunión de n personas y sea a_n el número de saludos que suceden entre las n personas si todas se saludan entre sí una, y sólo una, vez y ninguna se saluda a sí misma. Pensemos ahora en una reunión de $n-1$ personas ($n \geq 2$), entonces el número de saludos de dicho tipo es a_{n-1}. Imaginemos finalmente que una nueva persona, la persona n, acude a la reunión, saludará a las $n-1$ personas de ésta.

Subyace el principio de la adición.

0. *Formalización del principio de la adición.*

Para poder aplicar el principio de la adición debemos definir dos sucesos incompatibles, a saber:

$S_0 \leftrightharpoons$ en un grupo de $n-1$ personas, se saludan dos personas;

$S_1 \leftrightharpoons$ una persona nueva (la persona n) saluda a una de las $n-1$ personas anteriores;

que son incompatibles, puesto que la persona nueva no está entre las $n-1$ anteriores.

1. *De las formas de suceder los sucesos.*

Por lo comentado anteriormente:

a. el suceso S_0 sucede de a_{n-1} formas distintas;

b. el suceso S_1 sucede de $n-1$ formas distintas.

Observación.— Aunque es bastante intuitivo, pudiésemos también formalizar esto último por el principio de la adición, con los sucesos $S_i^1 \leftrightharpoons$ la persona n saluda a la persona i de la reunión de $n-1$ personas (sucesos incompatibles dos a dos por ser las personas diferentes), ya que cada uno de estos sucesos sucede de una única forma y nuestro interés radica en conocer el número de formas en que sucede el suceso unión, $\#(S_1^1 \cup S_2^1 \cup \ldots \cup S_{n-1}^1)$, esto es, $\#S_1$, que por el principio de la adición es $\#S_1^1 + \#S_2^1 + \cdots + \#S_{n-1}^1 = 1 + 1 + \cdots + 1 = n$.

2. *Aplicación del principio de la adición.*

Nuestro interés es averiguar el número de formas en que sucede el suceso unión $S_0 \cup S_1$. Como hemos dicho ya, son sucesos incompatibles dos a dos, así que es admisible aplicar el principio de la adición. Notando por $\#X$ el número de formas en que sucede un suceso X,

$$\begin{aligned} \#(S_0 \cup S_1) &= \#S_0 + \#S_1 \\ &= a_{n-1} + (n-1). \end{aligned}$$

Observemos que $\#(S_0 \cup S_1)$ no es otro que a_n.

Por todo esto, la situación descrita puede ser modelizada por la ecuación en diferencias

$$a_n = a_{n-1} + (n-1) \quad (2 \leq n),$$

que convenientemente reordenada queda

$$a_n - a_{n-1} = n - 1 \quad (2 \leq n). \tag{20.47}$$

II. *Propuesta de un problema de valores iniciales (PVI)*.

Exploramos algunos primeros valores iniciales:

- $a_0 = 0$ (no hay personas, no hay saludos);
- $a_1 = 0$ (ninguna persona se saluda a sí misma);
- $a_2 = 1$ (dos personas se saludan sólo una vez).

Observamos, pues, que la sucesión que buscamos tiene como definición implícita *el problema de valores iniciales de ecuaciones en diferencias* (PVI)

$$\begin{aligned} a_n - a_{n-1} = n - 1 \quad (2 \leq n), \\ a_0 = 0. \end{aligned}$$

III. *Demostración de que dicho PVI tiene solución única*.

Se trata de una ecuación en diferencias de orden uno ($|n - (n-1)| = 1$), lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, tiene una única solución.

Como el orden de (20.47) es uno, necesitamos sólo un valor inicial. Precisamente es lo que tenemos, por lo tanto, del teorema CERO se sigue que existe una única solución.

IV. *Cálculo de las raíces características pertinentes*.

Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico correspondiente a la homogénea asociada (la propia ED de partida en este caso) es $r-1$, siendo $r=1$ la única raíz característica simple, esto es, con multiplicidad 1.

v. *Obtención de las soluciones de las ED concernientes*.

0. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

   De lo anterior, por el teorema 20.14 (pág. 1325 de esta edición) (teorema TRES), *esta solución general* es:

$$a_n^{(h)} = c \cdot 1^n \quad (c \in \mathbb{R}),$$

   en definitiva,

$$a_n^{(h)} = c \quad (c \in \mathbb{R}). \tag{20.48}$$

1. *Obtención de una solución particular de la completa* (Paso III de ARED5).

   La forma general del término no homogéneo $F(n)$ que hemos estudiado en el teorema SEIS es

$$F(n) = (b_t n^t + b_{t-1} n^{t-1} + \cdots + b_1 n + b_0) \cdot s^n,$$

   con $b_t, b_{t-1}, \ldots, b_1, b_0, s \in \mathbb{R}$, en nuestro caso,

$$F(n) = n - 1,$$

   que reescribimos en la forma general:

$$F(n) = (1 \cdot n + (-1)) \cdot 1^n,$$

   esto es, el caso particular para $t=1$, $b_1=1$, $b_0=-1$ y $s=1$, y según el teorema 20.17 (pág. 1328 de esta edición) (teorema SEIS), como $s=1$ es una raíz característica de la homogénea asociada, con multiplicidad $m_s=1$, entonces existe una solución particular $\{a_n^{(p)}\}$ de la completa, de la forma

$$n^{m_s}(p_t n^t + p_{t-1} n^{t-1} + \cdots + p_1 n + p_0) \cdot s^n,$$

   con $p_t, p_{t-1}, \ldots, p_1, p_0, s \in \mathbb{R}$, en nuestro caso,

$$n^1 \cdot (p_1 n + p_0) \cdot 1^n,$$

   esto es,

$$a_n^{(p)} = n \cdot (p_1 n + p_0).$$

Como $\{a_n^{(p)}\}$ satisface (20.47), para $n \geq 1$,

$$a_n^{(p)} = a_{n-1}^{(p)} + (n-1),$$

esto es,

$$n \cdot (p_1 n + p_0) = (n-1) \cdot (p_1(n-1) + p_0) + (n-1),$$

que no es otra cosa que la igualdad de polinomios en n,

$$p_1 n^2 + p_0 n = p_1 n^2 + (p_0 - 2p_1 + 1)n + (p_1 - p_0 - 1),$$

de la cual, precisamente por definición de igualdad de polinomios, se tiene la igualdad de coeficientes:

$$\begin{aligned} p_1 &= p_1, \\ p_0 &= p_0 - 2p_1 + 1, \\ 0 &= p_1 - p_0 - 1. \end{aligned}$$

De aquí,

$$\begin{aligned} p_0 &= -\frac{1}{2}, \\ p_1 &= \frac{1}{2}, \end{aligned}$$

por lo que

$$a_n^{(p)} = n \cdot \left(\frac{n}{2} - \frac{1}{2}\right),$$

esto es, una solución particular de la no homogénea es

$$a_n^{(p)} = \frac{n(n-1)}{2}.$$

2. *Obtención de la solución general de la completa* (Paso IV de ARED5).

   Por el teorema 20.16 (pág. 1328 de esta edición) (teorema CINCO), la solución general $\{a_n\}$ de la completa es $\{a_n^{(h)} + a_n^{(p)}\}$, esto es, $\{a_n\}$ está definida por

$$a_n = c + n \cdot \left(\frac{n}{2} - \frac{1}{2}\right) \quad (c \in \mathbb{R}),$$

   esto es, por

$$a_n = c + \frac{(n-1)n}{2} \quad (c \in \mathbb{R}). \tag{20.49}$$

VI. *Obtención de la solución del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo el valor inicial $a_0 = 0$ (no hay personas, no hay saludos) en (20.49) tenemos

$$a_0 = 0 = c + \frac{(0-1)\cdot 0}{2},$$

de donde $c = 0$ y, por lo tanto, la única solución del problema de valores iniciales es

$$a_n = \frac{(n-1)n}{2}.$$

Solución.— El número de saludos que suceden entre n personas si todas se saludan entre sí una, y sólo una, vez y ninguna persona se saluda a sí misma, es $(n-1)n/2$. ■

Observación 20.5.18.— La sucesión $\{a_n\}$ está catalogada como la sucesión A161680 en la OEIS[44].

El término $n+1$ de esta sucesión es precisamente el enésimo número triangular, esto es,

$$a_{n+1} = T_n,$$

donde T_n es la sucesión de los números triangulares[45], que se definen tradicionalmente como la solución única del PVI (comparémosla con la de a_n)

$$T_n = T_{n-1} + n \quad (n \geq 1),$$
$$T_0 = 0,$$

y cuya expresión explícita más frecuente es

$$T_n = \frac{n(n+1)}{2}.$$

Los números triangulares están catalogados como la sucesión A000217 en la OEIS[46].

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
a_n	0	0	1	3	6	10	15	21	28	36	...
T_n	0	1	3	6	10	15	21	28	36	45	...

Observación 20.5.19.— *Cfr. supra* ejemplo 612 (pág. 1137 de esta edición).

Actividad 20.10

Calculemos el número de saludos tratado que ocurren en un grupo de n personas, desde $n = 1$ a $n = 23$, mediante un programa en el lenguaje de programación Sage que solucione el

44 *Vid.* https://oeis.org/A161680.
45 *Vid. v. gr.* https://es.wikipedia.org/wiki/N%C3%BAmero_triangular.
46 *Vid.* https://oeis.org/A000217.

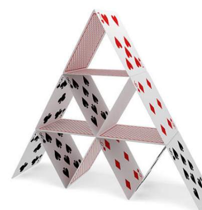
problema de valores iniciales

$$a_n - a_{n-1} = n - 1 \qquad (1 \leq n),$$
$$a_1 = 0.$$

Ejemplo 750

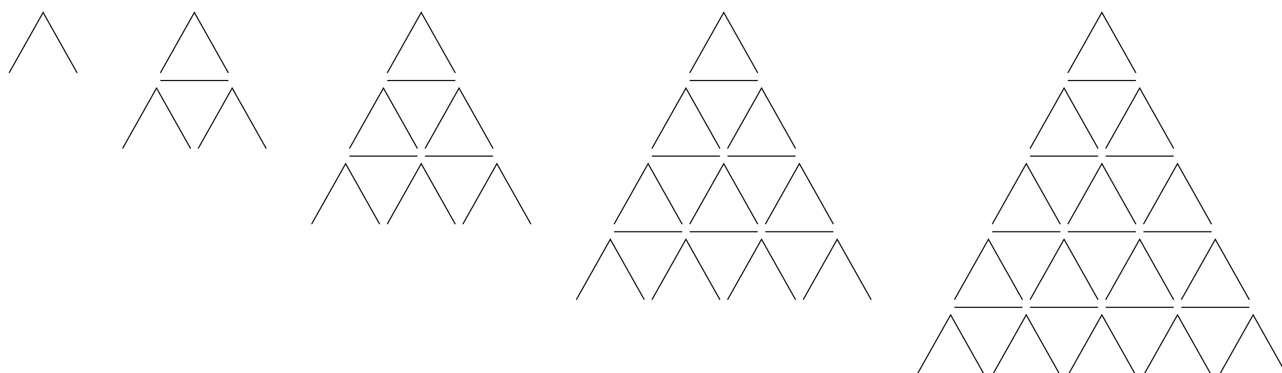
¿Cuántas cartas son necesarias para formar un castillo de naipes de n pisos? En la imagen, apreciamos que hicieron falta 15 para formar un castillo de naipes de 3 pisos.

[EFE 29.6.2018:7].



Resolución.—

1. *Propuesta de una ecuación en diferencias (ED) o más.*



En la figura vemos los casos desde $n = 1$ a $n = 5$. Numeramos los pisos en orden ascendente de arriba abajo. Observamos que en el piso n hay:

- dos nodos terminales extremos, esto es, un nodo terminal izquierdo y un nodo terminal derecho, que generan cada uno dos cartas en el piso siguiente hacia abajo;
- $(n-1)$ nodos terminales interiores que generan cada uno dos cartas en el piso siguiente hacia abajo, esto es, un total de $2 \cdot (n-1)$ cartas;
- $(n+1)$ nodos terminales que generan n cartas horizontales —de techo— en el piso siguiente hacia abajo.

Designemos N_n para representar el número de cartas en un castillo de naipes de n pisos, entonces

$$N_{n+1} = N_n + 2 \cdot 2 + 2 \cdot (n-1) + n,$$

o bien,

$$N_n = N_{n-1} + 2 \cdot 2 + 2 \cdot (n-2) + n - 1$$

y, en definitiva,

$$N_n = N_{n-1} + 3n - 1,$$

con $n > 1$, es una ecuación en diferencias para N_n.

De hecho, se trata de una ecuación en diferencias de orden 1, lineal, no homogénea y de coeficientes constantes.

Sin duda, somos capaces de comprobar los casos representados en la figura:

$$\begin{aligned} N_1 &= 2, \\ N_2 &= 7 &&= N_1 + 3 \cdot 2 - 1, \\ N_3 &= 15 &&= N_2 + 3 \cdot 3 - 1, \\ N_4 &= 26 &&= N_3 + 3 \cdot 4 - 1, \\ N_5 &= 40 &&= N_4 + 3 \cdot 5 - 1. \end{aligned}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Con $N_1 = 2$ como condición inicial, conformamos *el problema de valores iniciales*

$$\begin{gathered} N_n - N_{n-1} = 3n - 1 \qquad (n > 1), \\ N_1 = 2, \end{gathered}$$

que resolvemos a continuación con la teoría estudiada.

Vía 0.

(en la observación 20.5.21 [pág. 1375 de esta edición] estudiamos una vía alternativa).

I. *Demostración de que dicho PVI tiene solución única.*

Se trata de una ecuación en diferencias de orden uno, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, tiene una única solución. Como $N_n - N_{n-1} = 3n - 1$ es de orden uno, necesitamos sólo un valor inicial. Y lo tenemos: $N_1 = 2$.

II. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). Dicha ecuación homogénea asociada es

$$N_n - N_{n-1} = 0.$$

El polinomio característico asociado a ella es

$$x - 1$$

siendo

$$r_0 = 1$$

la raíz característica simple, esto es, con multiplicidad 1.

III. *Obtención de las soluciones de las ED concernientes.*

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De lo anterior, por un teorema conocido —*cfr. supra* teorema 20.12 (pág. 1314 de esta edición) (teorema UNO)—, *la solución general* es

$$N_n^{(h)} = c \cdot 1^n \qquad (c \in \mathbb{R}),$$

esto es,

$$N_n^{(h)} = c \qquad (c \in \mathbb{R}). \tag{20.50}$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

La hallamos mediante el método de los coeficientes indeterminados. En la presente cuestión, $F(n) = 3n - 1$, por lo que $b_0 = 1$, $b_1 = 3$ y $s = 1$. Como s es raíz de la homogénea asociada con multiplicidad 1, entonces por el teorema 20.17 (pág. 1328 de esta edición) (teorema SEIS), existe una solución particular de la completa de la forma $n^1(p_1 n + p_0)1^n$, esto es, de la forma $p_1 n^2 + p_0 n$.

Sustituyendo en la completa:

$$\begin{aligned}(p_1 n^2 + p_0 n) - (p_1(n-1)^2 + p_0(n-1)) &= 3n - 1,\\ p_1 n^2 + p_0 n - p_1 n^2 + 2p_1 n - p_1 - p_0 n + p_0 &= 3n - 1,\\ 2p_1 n - p_1 + p_0 &= 3n - 1,\end{aligned}$$

de donde

$$\begin{aligned}p_0 &= \frac{1}{2},\\ p_1 &= \frac{3}{2},\end{aligned}$$

por lo que una solución particular de la completa es

$$N_n^{(p)} = \frac{3}{2}n^2 + \frac{1}{2}n. \tag{20.51}$$

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

La solución general de la completa es la suma de la solución general de la homogénea asociada y una solución particular de la completa, esto es,

$$N_n = N_n^{(h)} + N_n^{(p)}. \tag{20.52}$$

Sustituyendo (20.50) y (20.51) en (20.52), obtenemos

$$N_n = c + \frac{3}{2}n^2 + \frac{1}{2}n. \tag{20.53}$$

IV. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Para ello, como es una ecuación de orden uno, se necesita un valor inicial, en este caso, $N_1 = 2$. Así,

$$N_1 = 2 = c + \frac{3}{2} \cdot 1^2 + \frac{1}{2} \cdot 1,$$

de donde

$$c = 0. \tag{20.54}$$

Sustituyendo el valor inicial (20.54) en (20.53), obtenemos la solución única buscada en forma explícita

$$N_n = \frac{3}{2}n^2 + \frac{1}{2}n.$$

Solución.— El número de cartas necesarias para formar un castillo de naipes de n pisos ($n \in \mathbb{N}$) viene dado por $(3n^2 + n)/2$. ■

Observación 20.5.20.— Notemos que la solución tiene sentido para cero, esto es, $N_0 = 0$, es decir, en el piso 0 no hay cartas —por construcción, no hay cartas horizontales (cartas en la «base») en ningún piso—. De hecho, $\{N_n\}$ es la sucesión de los *segundos números pentagonales*, ${}_2p_n$), catalogada como la sucesión A005449 en la OEIS[47], donde encontramos diversas fórmulas e interpretaciones.

Por otro lado, tenemos la sucesión de los *números pentagonales*, $\langle p_n \rangle$, que está catalogada como la sucesión A000326 en la OEIS[48] y la sucesión de los *números pentagonales generalizados* $\langle {}_g p_n \rangle$, catalogada como la sucesión A001318 en la OEIS[49].

Notemos que ${}_2p_n = {}_g p_{2n}$ y que $p_n = {}_g p_{2n-1} (1 \leq n)$ y $p_0 = 0$.

[47] *Vid.* https://oeis.org/A005449.
[48] *Vid.* https://oeis.org/A000326.
[49] *Vid.* https://oeis.org/A001318.

Enumerativamente:

n	0		1		2		3		4		5		6		7		8		9	...
$N_n = {}_2p_n$	0		2		7		15		26		40		57		77		100		126	...
p_n	0		1		5		12		22		35		51		70		92		117	...
${}_gp_m$	0	1	2	5	7	12	15	22	26	35	40	51	57	70	77	92	100	117	126	...
m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	...

Observación 20.5.21.— Una vez resuelto II, esto es, obtenido el problema de valores iniciales de ecuaciones en diferencias y demostrado que tiene solución única, es posible solucionarlo por diferentes caminos. En la vía empleada en la resolución no nos ha hecho falta demostrar nada, ya que es consecuencia de la aplicación directa de teoremas. A continuación, vemos otra vía, a partir de expandir, en la que sí tendremos que demostrar, en este caso por inducción débil, pues es resultado de una intuición.

Vía 1.

Tenemos la sucesión $\{N_n\}$ definida inductivamente por

$$N_n - N_{n-1} = 3n - 1 \qquad (n > 1), \tag{20.55}$$

a partir de la que expandiendo intentaremos intuir la solución que finalmente deberemos demostrar que lo es; en definitiva, aplicaremos sustitución hacia atrás (SHT) (*cfr. supra* § 20.3.1 [pág. 1305 de esta edición]).

0. *Expansión*.

   Aplicamos la definición inductiva (20.55) reiteradamente:

$$\begin{aligned} N_n &= N_{n-1} + 3n - 1 \\ &= (N_{n-2} + 3(n-1) - 1) + 3n - 1 && = N_{n-2} + 2\cdot 3n - 3\cdot 1 - 2 \\ &= (N_{n-3} + 3(n-2) - 1) + 2\cdot 3n - 3\cdot 1 - 2 && = N_{n-3} + 3\cdot 3n - 3\cdot(1+2) - 3 \\ &= (N_{n-4} + 3(n-3) - 1) + 3\cdot 3n - 3\cdot(1+2) - 3 && = N_{n-4} + 4\cdot 3n - 3\cdot(1+2+3) - 4 \end{aligned}$$

   y así sucesivamente.

1. *Intuición*.

   A partir de la expansión anterior, intuimos, para $k \in \mathbb{N}$,

$$N_n = N_{n-k} + k\cdot 3n - 3\cdot(1+2+3+\ldots+(k-1)) - k,$$

   que por ser $1+2+3+\ldots+(k-1)$ la suma parcial de $k-1$ términos de una progresión aritmética de diferencia 1, queda

$$N_n = N_{n-k} + k\cdot 3\frac{k(k-1)}{2} - k.$$

   Los subíndices de N son n, $n-1$, $n-2$, ..., es decir, una sucesión decreciente que termina en N_1, esto es, que tiene como condición de terminación $n-k=1$, equivalentemente, $k = n-1$.

Así:

$$\begin{aligned}N_n &= N_1 + (n-1)\cdot 3n - \frac{3}{2}(n-1)(n-2) - (n-1)\\ &= 2 + 3n^2 - 3n - \frac{3}{2}(n^2 - 3n + 2) - n + 1\\ &= 2 + \left(3 - \frac{3}{2}\right) n^2 + \left(-3 + \frac{9}{2}\right) n - 3 - n + 1\\ &= \frac{3}{2}n^2 + \frac{3}{2}n - n;\end{aligned}$$

en definitiva,

$$N_n = \frac{3}{2}n^2 + \frac{1}{2}n.$$

2. *Demostración*.

Utilizaremos inducción débil. Sea $P(n) \leftrightharpoons N_n = \frac{3}{2}n^2 + \frac{1}{2}n$. Nos proponemos demostrar que $\forall n \in \mathbb{N}, P(n)$. Para ello, apliquemos el teorema 16.0 (pág. 805 de esta edición) (teorema de inducción débil).

Caso base (ID_0).— Para $n = 1$, por un lado, $N_1 = 2$ (es la condición inicial) y, por otro, $\frac{3}{2}\cdot 1^2 + \frac{1}{2} = 2$; en otras palabras, se satisface $P(1)$.

Paso inductivo (ID_1).— Supongamos $P(k)$ y demostremos $P(k+1)$, esto es, supongamos que $N_k = \frac{3}{2}k^2 + \frac{1}{2}k$ (*hipótesis inductiva*) y demostremos que $N_{k+1} = \frac{3}{2}(k+1)^2 + \frac{1}{2}(k+1)$ (*tesis inductiva*); en efecto,

$$\begin{aligned}N_{k+1} &= N_k + 3(k+1) - 1 && \text{[por definición inductiva]}\\ &= \frac{3}{2}k^2 + \frac{1}{2}k + 3k + 3 - 1 && \text{[por hipótesis inductiva]}\\ &= \frac{3}{2}k^2 + \frac{1}{2}k + 3k + 2\\ &= \frac{3}{2}k^2 + 3k + \frac{3}{2} + \frac{1}{2}k + \frac{1}{2}\\ &= \frac{3}{2}(k+1)^2 + \frac{1}{2}(k+1),\end{aligned}$$

en otras palabras, se satisface $P(k+1)$.

Conclusión ($\mathrm{ID}_0 \wedge \mathrm{ID}_1$).— Como se satisfacen el caso base y el paso inductivo, entonces, por el teorema 16.0 (pág. 805 de esta edición) (teorema de inducción débil) se tiene lo buscado, a saber, que

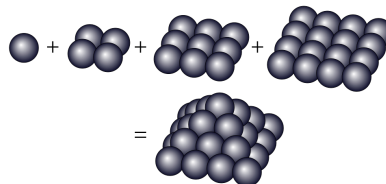
$$(\forall n \in \mathbb{N})\ \left(N_n = \frac{3}{2}n^2 + \frac{1}{2}n\right),$$

siendo éste el número de cartas necesarias para formar un castillo de naipes de n pisos, como ya vimos en la vía 0 de resolución. ■

Ejemplo 751

¿Cuántas bolas son necesarias para formar una pirámide de base cuadrada de n pisos? Apreciamos en la imagen que hicieron falta 30, esto es, $1 + 4 + 9 + 16$, para formar una pirámide de base cuadrada de cuatro pisos.

[EFO 3.6.2019:6].



Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más.*

La base de una pirámide de base cuadrada de n pisos tiene $n \cdot n = n^2$ bolas y sobre dicha base se asienta una pirámide de base cuadrada de $n - 1$ pisos. Si b_n designa el número de bolas de una pirámide de n pisos, entonces la situación descrita puede ser modelizada por la ecuación en diferencias

$$b_n = b_{n-1} + n^2, \tag{20.56}$$

que convenientemente reordenada es

$$b_n - b_{n-1} = n^2, \tag{20.57}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Con $b_1 = 1$ (una pirámide cuadrada de un piso tiene sólo una bola) como condición inicial, conformamos *el problema de valores iniciales*

$$\begin{aligned} b_n - b_{n-1} &= n^2 \qquad (n > 1), \\ b_1 &= 1, \end{aligned}$$

que resolveremos con la teoría estudiada.

III. *Demostración de que dicho PVI tiene solución única*

Se trata de una ecuación en diferencias de orden uno, lineal, no homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, tiene una única solución. Como $b_n - b_{n-1} = n^2$ es de orden uno, necesitamos sólo un valor inicial. Y lo tenemos: $b_1 = 1$.

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). Dicha ecuación homogénea asociada de (20.57) es

$$b_n - b_{n-1} = 0. \tag{20.58}$$

El polinomio característico asociado a dicha ED es $r - 1$, siendo 1 su única raíz característica, que es simple (multiplicidad 1).

V. *Obtención de las soluciones de las ED concernientes*.

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De acuerdo con el teorema 20.15 (pág. 1327 de esta edición) (teorema CUATRO), la solución general de la homogénea asociada es

$$b_n^{(h)} = \alpha 1^n = \alpha \quad (\alpha \in \mathbb{R}). \tag{20.59}$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

La parte no homogénea ($F(n) = n^2$) es un polinomio de grado 2 que reescribimos como $F(n) = n^2 1^n$, de manera que en el teorema 20.17 (pág. 1328 de esta edición) (teorema SEIS), $t = 2$, $b_2 = 1$ y $s = 1$ y como $s = 1$ es raíz característica con multiplicidad $m_1 = 1$, entonces, según dicho teorema, existe una solución de la no homogénea de la forma

$$n^{m_1} \cdot (p_t n^t + p_{t-1} n^{t-1} + \ldots + p_1 n + p_0) \cdot 1^n, \tag{20.60}$$

en nuestro caso,

$$n^1 \cdot (p_2 n^2 + p_1 n + p_0) \cdot 1^n, \tag{20.61}$$

esto es,

$$b_n^{(p)} = p_2 n^3 + p_1 n^2 + p_0 n. \tag{20.62}$$

Ahora, como $b_n^{(p)}$ satisface la no homogénea (20.56), entonces, sustituyendo en ella,

$$\begin{aligned} p_2 n^3 + p_1 n^2 + p_0 n = p_2(n-1)^3 + p_1(n-1)^2 + \\ p_0(n-1) + n^2, \end{aligned} \tag{20.63}$$

de donde, simplificando y reordenando convenientemente queda:

$$3p_2 n^2 + (2p_1 - 3p_2)n + (p_2 - p_1 + p_0) = n^2, \tag{20.64}$$

y ahora, igualando los coeficientes de los términos correspondientes:

$$3p_2 = 1, \tag{20.65}$$

$$2p_1 - 3p_2 = 0, \tag{20.66}$$

$$p_2 - p_1 + p_0 = 0, \tag{20.67}$$

se deduce que:

$$p_2 = \frac{1}{3}, \tag{20.68}$$
$$p_1 = \frac{1}{2}, \tag{20.69}$$
$$p_0 = \frac{1}{6}, \tag{20.70}$$

de donde, sustituyendo en (20.78), tenemos, en definitiva, que una solución particular de la no homogénea es:

$$b_n^{(p)} = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n. \tag{20.71}$$

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

Se tiene entonces que la solución general de la no homogénea es (*vid.* teorema 5) $\{b_n^{(h)}\} + \{b_n^{(p)}\}$, esto es,

$$b_n = \alpha + \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n \quad (\alpha \in \mathbb{R}), \tag{20.72}$$

esto es, un número infinito no numerable de sucesiones, una para cada $\alpha \in \mathbb{R}$.

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Para hallar por fin la solución particular única de la cuestión en estudio, como es una ecuación de orden uno, vimos que se necesita un valor inicial, que en este ejemplo es $b_1 = 1$. Así,

$$b_1 = 1 = \alpha + \frac{1}{3} \cdot 1^3 + \frac{1}{2} \cdot 1^2 + \frac{1}{6} \cdot 1,$$

de donde, $\alpha = 0$.

Solución.— El número de bolas necesarias para formar una pirámide de base cuadrada de n pisos es

$$b_n = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n \quad (0 < n). \qquad \blacksquare$$

Observación 20.5.22.— La sucesión $\{b_n\}$ está catalogada como la sucesión A000330 en la OEIS[50]; se trata de la sucesión $\langle Y_5^{(3)}(n) \rangle$ de los *números piramidales cuadrados*[51].

Enumerativamente:

Observación 20.5.23.— También pudiésemos haberlo resuelto por las estrategias de sustitución o por la telescópica. Dichas resoluciones suponen conocer la suma parcial de la serie de los cua-

[50] *Vid*. https://oeis.org/A000330.

[51] *Vid. v. gr.* https://oeis.org/wiki/Pyramidal_numbers; https://es.wikipedia.org/wiki/N%C3%BAmero_piramidal_cuadrado.

drados —*cfr. supra* observación 20.1.5 (pág. 1299 de esta edición)—, a saber,

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

además de tener que demostrar la fórmula explícita obtenida para b_n, por ejemplo, mediante inducción débil.

Ejemplo 752

Supongamos que las únicas contraseñas válidas para un sistema informático son las palabras finitas de dígitos ternarios (base 3) que contienen un número par de ceros (se permiten ceros encabezando la palabra). Se pide que calculemos el número de contraseñas válidas de longitud n.

[EFE 25.6.2019:6], [EFE 19.1.2023:10], [SEL 13:9].

Resolución.—

1. *Propuesta de una ecuación en diferencias (ED) o más.*

Designemos c_n para representar el número de palabras ternarias de longitud n que contienen un número par de ceros. Para construir una ecuación en diferencias para c_n razonemos hacia atrás, observando una palabra ternaria de longitud n que contiene un número par de ceros. Pueden suceder tres casos:

0.°, que termine en 1, entonces la palabra ternaria de longitud $n-1$ que precede a dicho 1 contiene un número par de ceros, habiendo c_{n-1} de tales palabras;

1.°, que termine en 2, entonces la palabra ternaria de longitud $n-1$ que precede a dicho 2 contiene un número par de ceros, habiendo c_{n-1} de tales palabras, o

2.°, que termine en 0, entonces la palabra ternaria de longitud $n-1$ que precede a dicho 0 contiene un número *impar* de ceros; como hay un total de $VR(3, n-1) = 3^{n-1}$ palabras ternarias de longitud $n-1$—pues cada palabra ternaria es una aplicación sin restricciones de un conjunto de cardinal $n-1$ en el conjunto $\{0, 1, 2\}$—, se tiene que hay $3^{n-1} - c_{n-1}$ palabras ternarias de longitud $n-1$ que contienen un número impar de ceros.

Subyace el *principio de la adición*. Estos casos —sucesos, en realidad— se excluyen mutuamente —son incompatibles, ya que cada palabra sólo puede terminar en un número— y su unión es el suceso ser una contraseña válida de longitud n, entonces, por el principio de la adición, dicho suceso unión sucede de c_n formas distintas, donde

$$c_n = c_{n-1} + c_{n-1} + 3^{n-1} - c_{n-1}, \tag{20.73}$$

esto es, que, en definitiva, dicho número c_n de formas distintas viene dado como solución de

$$c_n - c_{n-1} - 3^{n-1} = 0. \tag{20.74}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Al ser la ecuación lineal no homogénea de coeficientes constantes y orden 1, por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), basta con un valor inicial para conformar un problema de valores iniciales de ecuaciones en diferencias que tenga una solución única. Resulta que hay dos palabras ternarias de longitud uno que contienen un número par de ceros, la palabra 1 y la palabra 2 (contienen cero ceros).

Observamos, pues, que la sucesión que buscamos tiene como definición implícita *el problema de valores iniciales de ecuaciones en diferencias*

$$\begin{aligned} c_n - c_{n-1} - 3^{n-1} &= 0 \qquad (n > 1), \\ c_1 &= 2. \end{aligned} \tag{20.75}$$

III. *Demostración de que dicho PVI tiene solución única.*

Se trata de una ecuación en diferencias de orden 1, lineal, no homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, *tiene una única solución.*

En los siguientes apartados deduciremos formalmente la solución única del PVI en forma explícita y demostraremos que efectivamente lo es. En el caso en estudio tenemos $k = 1$, el orden es uno y disponemos de una condición inicial.

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). La ecuación homogénea asociada de (20.74) es

$$c_n - c_{n-1} = 0. \tag{20.76}$$

El polinomio característico asociado a dicha ED es $x - 1$, siendo por tanto su única raíz característica $r = 1$, que es simple (multiplicidad 1).

V. *Obtención de las soluciones de las ED concernientes.*

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De lo anterior que por un teorema conocido —teorema 20.12 (pág. 1314 de esta edición) (teorema UNO) o teorema 20.15 (pág. 1327 de esta edición) (teorema CUATRO)— *la solución*

general es:

$$c_n^{(h)} = \alpha \cdot (1)^n = \alpha \qquad (\alpha \in \mathbb{R}). \tag{20.77}$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

La parte no homogénea ($F(n) = 3^{n-1}$) es una función exponencial que reescribimos como $F(n) = 3^{-1}3^n$, de manera que en el teorema 20.17 (pág. 1328 de esta edición) (teorema SEIS), $b_0 = 3^{-1}$ y $s = 3$ y como 3 no es raíz característica, según dicho teorema, una solución de la no homogénea es:

$$p_0 3^n. \tag{20.78}$$

Sustituyendo en la no homogénea:

$$p_0 3^n = p_0 3^{n-1} + 3^{n-1}, \tag{20.79}$$

de donde, simplificando y reordenando convenientemente queda:

$$3p_0 3^n = p_0 + 1, \tag{20.80}$$

se deduce que:

$$p_0 = \frac{1}{2}, \tag{20.81}$$

por lo que una solución particular de la no homogénea es:

$$c_n^{(p)} = \frac{1}{2}3^n. \tag{20.82}$$

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

Se tiene entonces que la solución general de la no homogénea es —*vid. supra* teorema 20.16 (pág. 1328 de esta edición) (teorema CINCO)—

$$\begin{aligned} c_n &= c_n^{(h)} + c_n^{(p)} &(20.83)\\ &= \alpha + \frac{1}{2}3^n \quad (\alpha \in \mathbb{R}). &(20.84) \end{aligned}$$

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Para ello, como es una ecuación de orden 1, necesitamos un único valor inicial, en este caso, $c_1 = 2$. Así:

$$c_1 = 2 = \alpha + \frac{1}{2}3^1, \tag{20.85}$$

de donde:

$$\alpha = \frac{1}{2}. \tag{20.86}$$

Sustituyendo (20.86) en (20.84), obtenemos la solución única en forma explícita buscada,

$$c_n = \frac{1}{2}\left(3^n + 1\right).$$

Solución.— El número de contraseñas válidas de longitud n que admite este sistema informático viene dado por

$$c_n = \frac{1}{2}\left(3^n + 1\right) \qquad (n > 0).$$

■

Observación 20.5.24.— Enumerativamente, la sucesión $\{c_n\}$ del ejemplo anterior es

n	0	1	2	3	4	5	6	7	8	9	...
c_n	1	2	5	14	41	122	365	1094	3281	9842	...

Esta sucesión está catalogada como la sucesión A007051 en la OEIS[52], donde encontramos diversas interpretaciones, fórmulas, referencias, enlaces, ejemplos, programas, referencias cruzadas y personas relacionadas con ella.

Observación 20.5.25.— Como sabemos, una vez resueltos los apartados I, II y III, esto es, obtenido el problema de valores iniciales de ecuaciones en diferencias y demostrado que tiene solución única, pudiésemos haberlo solucionado por cualquier otro método estudiado o conocido, sin olvidar que en algunos casos, como por ejemplo, si lo hubiésemos hecho mediante expansión, deberíamos demostrar el resultado seguramente mediante inducción. En nuestra resolución no hace falta, pues el resultado es consecuencia de la aplicación directa de teoremas —y no de una intuición—.

Veamos, por ejemplo, cómo resolver el ejemplo anterior por sustitución hacia atrás (SHT), esto es, expandiendo hacia atrás, intuyendo y demostrando lo intuido (EID). De las etapas de expansión e intuición, obtenemos:

$$\begin{aligned} c_n &= c_{n-1} + 3^{n-1} \\ &= c_{n-2} + 3^{n-2} + 3^{n-1} \\ &= c_{n-3} + 3^{n-3} + 3^{n-2} + 3^{n-1} \\ &\;\vdots \\ &= c_1 + 3^1 + 3^2 + \cdots + 3^{n-1} \\ &= 2 + \frac{3^n - 3}{3 - 1} \end{aligned}$$

[52] *Vid.* https://oeis.org/A007051.

[ya que la suma parcial S_n de los n primeros términos de una progresión geométrica $\{a_n\}$ de razón r y término inicial a_1 es $S_n = a_1 \cdot (r^n - 1)/(r-1)$; en nuestro caso, la suma de los $n-1$ primeros términos es $S_{n-1} = 3 \cdot (3^{n-1}-1)/(3-1)$, esto es, $S_{n-1} = (3^n - 3)/(3-1)$]

$$= \frac{4 + 3^n - 3}{2}$$
$$= \frac{1}{2}(3^n + 1).$$

Ahora, debemos demostrar que $\forall n \in \mathbb{Z}^+$, $c_n = (3^n + 1)/2$. Por ejemplo, mediante inducción débil. Para ello, apliquemos el teorema 16.0 (pág. 805 de esta edición) (teorema de inducción débil).

Caso base (ID_0).— Para $n = 1$, según lo que hemos intuido, $c_1 = (3^1 + 1)/2$, lo cual coincide con lo que dijimos en (20.75), a saber, que $c_1 = 2$ (la condición inicial); en otras palabras, se satisface $P(1)$.

Paso inductivo (ID_1).— Supongamos $P(k)$ y demostremos $P(k+1)$, esto es, supongamos que $c_k = \left(3^k + 1\right)/2$ (*hipótesis inductiva*) y demostremos que $c_{k+1} = \left(3^{k+1} + 1\right)/2$ (*tesis inductiva*); en efecto,

$$\begin{aligned} c_{k+1} &= c_k + 3^k \\ &= \frac{1}{2}\left(3^k + 1\right) + 3^k \\ &= \frac{1}{2}3^k + \frac{1}{2} + \frac{2}{2}3^k \\ &= \frac{3}{2}3^k + \frac{1}{2} \\ &= \frac{1}{2}\left(3 \cdot 3^k + 1\right) \\ &= \frac{1}{2}\left(3^{k+1} + 1\right). \end{aligned}$$

en otras palabras, se satisface $P(k+1)$.

Conclusión ($\mathrm{ID}_0 \wedge \mathrm{ID}_1$).— Como se satisfacen el caso base y el paso inductivo, entonces, por el teorema 16.0 (pág. 805 de esta edición) (teorema de inducción débil) se tiene lo buscado, a saber, que $\forall n \in \mathbb{Z}^+$,

$$c_n = \frac{1}{2}(3^n + 1).$$

Ejemplo 753

Sea la ecuación en diferencias $a_n - 3a_{n-1} + 2a_{n-2} = 0$, con $0 \leq n$, sabiendo que $a_2 = 2$ y $a_3 = 3$, ¿cuál es la solución de este problema de valores iniciales?

a. $a_n = n$.

b. $a_n = 2^{n-2} + 1$.

c. $a_n = 3^{n-2} - n + 3$.

d. $a_n = 4^{n-2} - 2n + 5$.

[TT], [EFE 3.7.2024:13] (tipo test).

Resolución.— Al ser una cuestión de opción múltiple con una única respuesta verdadera, probablemente lo más sencillo sea resolverlo por eliminación y comprobación: de la ecuación en diferencias que nos dan, $a_4 = 3a_3 - 2a_2$, de donde, sustituyendo los valores conocidos, $a_4 = 3 \cdot 3 - 2 \cdot 2$, esto es, $a_4 = 5$; las opciones a), c) y d) quedan eliminadas, pues, en ellas, $a_4 = 4$, $a_4 = 3^{4-2} - 4 + 3 = 8$ y $a_4 = 4^{4-2} - 2 \cdot 4 + 5 = 13$, respectivamente; comprobamos que en la opción b), $a_4 = 2^{4-2} + 1 = 5$.

Solución.— Opción b. ■

§ 20.5.2 Períodos de tiempo

Ejemplo 754

Consideremos una partícula que se desplaza horizontalmente con un movimiento acelerado. Supongamos que la distancia que recorre en cada segundo es el doble de la distancia que recorrió en el segundo previo. Si la partícula está inicialmente a una distancia de dos unidades de un punto fijo O y a una distancia de cinco unidades de O después de dos segundos, ¿cuál es la posición de la partícula respecto de O transcurridos n segundos?

[EFEC 25.6.2019:6], [EFO 24.5.2023:10], [EFE 3.7.2024:15] (tipo test), [EFO 27.5.2025:10], [EFE 18.6.2025:10].

Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más.*

Siendo p_t la posición de la partícula en el segundo t, la distancia recorrida del segundo $t-1$ al segundo t corresponde a la diferencia $p_t - p_{t-1}$, por lo que la situación descrita puede ser modelizada por la ecuación en diferencias

$$p_t - p_{t-1} = 2(p_{t-1} - p_{t-2}), \text{ para } t \geq 2,$$

que convenientemente reordenada queda

$$p_t - 3p_{t-1} + 2p_{t-2} = 0, \text{ para } t \geq 2. \tag{20.87}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Traducidos los datos en condiciones iniciales, se conforma el PVI:

$$p_t - 3p_{t-1} + 2p_{t-2} = 0, \text{ para } t \geq 2,$$
$$p_0 = 2,$$
$$p_2 = 5.$$

III. *Demostración de que dicho PVI tiene solución única*.

Se trata de una ecuación en diferencias de orden dos, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, tiene una única solución.

Como el orden de (20.87) es 2, necesitamos dos valores iniciales consecutivos. De $p_0 = 2$, $p_2 = 5$ y $p_2 - p_1 = 2(p_1 - p_0)$, se sigue que $5 - p_1 = 2(p_1 - 2)$, esto es, $p_1 = 3$, lo que nos permite reconfigurar equivalentemente el PVI:

$$p_t - 3p_{t-1} + 2p_{t-2} = 0, \text{ para } t \geq 2,$$

$$p_0 = 2, \tag{20.88}$$

$$p_1 = 3, \tag{20.89}$$

para el que según el teorema CERO existe una única solución.

IV. *Cálculo de las raíces características pertinentes*.

Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es $r^2 - 3r + 2$, siendo $r_0 = 1$ y $r_1 = 2$ las dos raices características simples, esto es, ambas con multiplicidad 1, y distintas.

V. *Obtención de las soluciones de las ED concernientes*.

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De lo anterior, por un teorema conocido —*cfr. supra* teorema 20.12 (pág. 1314 de esta edición) (teorema UNO)—, *la solución general* es

$$p_t = c_{r_0} + c_{r_1} 2^t \quad (\alpha_1, \alpha_2 \in \mathbb{R}). \tag{20.90}$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

VI. *Obtención de la solución del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo los dos valores iniciales consecutivos (20.88) y (20.89) en (20.90) tenemos el sistema de dos ecuaciones con dos incógnitas

$$p_0 = 2 = c_{r_0} + c_{r_1}2^0,$$
$$p_1 = 3 = c_{r_0} + c_{r_1}2^1,$$

cuya solución es

$$c_{r_0} = 1, \tag{20.91}$$
$$c_{r_1} = 1. \tag{20.92}$$

Sustituyendo (20.91) y (20.92) en (20.90), obtenemos la sucesión buscada, $p_t = 2^t + 1$.

Solución.— Transcurridos n segundos la posición de la partícula respecto de O viene dada por:

$$p_n = 2^n + 1.$$ ■

Observación 20.5.26.— Para todo n entero positivo, p_n es la *sucesión de* Pisot $\mathrm{L}(2,3)$, catalogada como la sucesión A000051 en la OEIS[53], donde $\mathrm{L}(x,y)$ es:

$$a_0 = x,$$
$$a_1 = y,$$
$$a_n = \left\lceil \frac{a_{n-1}^2}{a_{n-2}} \right\rceil.$$

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
$L(2,3)_n$	2	3	5	9	17	33	65	129	257	513	...

Observación 20.5.27.— *Cfr. infra* ejemplo 754 (pág. 1385 de esta edición).

[53] *Vid*. https://oeis.org/A000051.

Ejemplo 755

Como en el ejemplo 747 (pág. 1362 de esta edición), sea el arenero de un experimento web con una población de bots autorreplicantes malignos tal que no existen factores externos que modifiquen su crecimiento. Supongamos ahora que la población crece el doble, en cada período de tiempo que transcurre entre dos medidas, de lo que creció en el período inmediatamente anterior. Calculemos el número de bots en un instante arbitrario de tiempo t.

[EFE 29.6.2018:8], [EFO 20.5.2022:10], [SEL 13:7b].

Resolución.— Esta cuestión es equivalente a la resuelta en el ejemplo 754 (pág. 1385 de esta edición), salvo que aquí no se tienen condiciones iniciales. Como allí, la solución general es

$$p_t = c_1 2^t + c_0 \quad (c_0, c_1 \in \mathbb{R}). \tag{20.93}$$

Solución.— El número de bots en un instante de tiempo t es $y_t = c_1 2^t + c_0$, esto es, está en función de dos parámetros, $c_0, c_1 \in \mathbb{R}$. Si conociésemos las dos medidas iniciales y_0 e y_1, entonces conoceríamos los números reales c_0 y c_1 y, por lo tanto, sabríamos cuál es la única función de la familia anterior que proporciona el valor del número de bots en el instante t. ■

Ejemplo 756

En una simulación computacional predictiva estudiamos una población de entes futuros restringida a un área en la que se supone que salvo se concrete algo en contra, no existen factores externos que afecten a su crecimiento. Supongamos que en dicha área, en cada período de tiempo que transcurre entre dos medidas: a) la población crece el doble de lo que creció en el período inmediatamente anterior, b) abandonan la población tantos entes como un cuarto de la población inicial del período inmediatamente anterior, y c) se incorporan a la población 4 entes del exterior. Supongamos asimismo una población inicial de 3 entes y que el primer año se llega a 7 entes. Calculemos el número de entes en un instante arbitrario de tiempo t.

[EPF 14.5.2019:6].

Resolución.—

1. *Propuesta de una ecuación en diferencias (ED) o más.*

   Sea $y_t \coloneqq$ número de entes en el instante de tiempo t.

Observemos que si el período de tiempo que transcurre entre dos medidas es $y_{t+1} - y_t$, el período inmediatamente siguiente es $y_{t+2} - y_{t+1}$.

Así, podemos modelizar la situación descrita por la ecuación en diferencias

$$y_{t+2} - y_{t+1} = 2(y_{t+1} - y_t) + 4 - \frac{y_t}{4},$$

que convenientemente reordenada queda:

$$y_{t+2} - 3y_{t+1} + \frac{9}{4}y_t - 4 = 0,$$

o, si lo preferimos:

$$y_t - 3y_{t-1} + \frac{9}{4}y_{t-2} = 4. \tag{20.94}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

El hecho de que la población inicial sea de 3 entes y que el primer año se llegue a 7 entes se traduce en las condiciones iniciales (de contorno) $y_0 = 3$ e $y_1 = 7$ y, por tanto, en el PVI

$$\begin{aligned} y_t - 3y_{t-1} + \frac{9}{4}y_{t-2} &= 4, \\ y_0 &= 3, \\ y_1 &= 7. \end{aligned}$$

III. *Demostración de que dicho PVI tiene solución única.*

Se trata de una ecuación en diferencias de orden dos, lineal, no homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, tiene una única solución. Como el orden de (20.94) es dos, necesitamos dos valores iniciales consecutivos. Los tenemos: $y_0 = 3$ e $y_1 = 7$.

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). Dicha homogénea asociada es

$$y_t - 3y_{t-1} + \frac{9}{4}y_{t-2} = 0. \tag{20.95}$$

Su polinomio característico es $r^2 - 3r + 9/4$, siendo $3/2$ la raíz característica doble (multiplicidad 2).

V. *Obtención de las soluciones de las ED concernientes.*

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

La solución general de la homogénea asociada es

$$y_t^{(h)} = \alpha_1 \left(\frac{3}{2}\right)^t + \alpha_2 t \left(\frac{3}{2}\right)^t. \tag{20.96}$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

Como la parte no homogénea es una constante (4) y 1 no es raíz característica, la solución será polinómica de grado 0, esto es una constante; sea A dicha constante. Así, sustituyendo en la no homogénea:

$$A - 3A + \frac{9}{4}A - 4 = 0, \tag{20.97}$$

deducimos que $A = 16$, por lo que una solución particular de la no homogénea es $y_t^{(p)} = 16$.

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

Se tiene entonces que la solución general de la no homogénea es:

$$y_t = \alpha_1 \left(\frac{3}{2}\right)^t + \alpha_2 t \left(\frac{3}{2}\right)^t + 16. \tag{20.98}$$

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Hallemos finalmente la solución (particular) de la cuestión. Para ello, como es una ecuación de orden 2, se necesitan dos valores iniciales consecutivos, los cuales, como hemos visto, son proporcionados en el enunciado. Así:

$$y_0 = 3 = \alpha_1 \cdot \left(\frac{3}{2}\right)^0 + \alpha_2 \cdot 0 \cdot \left(\frac{3}{2}\right)^0 + 16, \tag{20.99}$$

$$y_1 = 7 = \alpha_1 \cdot \left(\frac{3}{2}\right)^1 + \alpha_2 \cdot 1 \cdot \left(\frac{3}{2}\right)^1 + 16, \tag{20.100}$$

de donde:

$$\alpha_1 = -13, \tag{20.101}$$

$$\alpha_2 = 7. \tag{20.102}$$

Solución.— En la población descrita en el enunciado, el número de entes en un instante de tiempo t viene dado por

$$y_t = (7t - 13)\left(\frac{3}{2}\right)^t + 16.$$ ■

Ejemplo 757

Como en el ejemplo 755 (pág. 1388 de esta edición), sea el arenero de un experimento web con una población de bots autorreplicantes malignos tal que no existen factores externos que modifiquen su crecimiento. Supongamos ahora que la población crece el triple, en cada período de tiempo que transcurre entre dos medidas, de lo que creció en el período inmediatamente anterior. Calculemos el número de bots en un instante arbitrario de tiempo t.

Resolución.—

I. *Propuesta de una ecuación en diferencias (ED) o más.*

Sea b_t la población (el número) de bots autorreplicantes malignos en el instante t en el que se toma una medida.

De nuevo aquí se habla del crecimiento relativo de la población en el período de tiempo que transcurre entre dos medidas $(t, t+1)$ y en el período de tiempo inmediatamente anterior $(t-1, t)$, si bien en esta ocasión se asegura que el primero es el triple del segundo.

El crecimiento de la población en el período $(t, t+1)$ es la diferencia $b_{t+1} - b_t$ y el crecimiento poblacional en el período $(t-1, t)$ es la diferencia $b_t - b_{t-1}$, por tanto, lo que dice el enunciado es que

$$b_{t+1} - b_t = 3 \cdot (b_t - b_{t-1}),$$

de donde, simplificando,

$$b_{t+1} - 4b_t + 3b_{t-1} = 0,$$

o en forma estándar,

$$b_t - 4b_{t-1} + 3b_{t-2} = 0. \tag{20.103}$$

II. *Propuesta de un problema de valores iniciales (PVI).*

El ejemplo 747 (pág. 1362 de esta edición), en el que últimamente se basa éste, nos informa de que partimos de una población inicial de cien bots, en otras palabras, tenemos un valor inicial $b_0 = 100$, por lo que el PVI es

$$\begin{aligned} b_t - 4b_{t-1} + 3b_{t-2} &= 0, \\ b_0 &= 100. \end{aligned}$$

III. *Demostración de que dicho PVI tiene solución única.*

Se trata de una ecuación en diferencias de orden dos, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un pro-

blema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, tiene una única solución. Como el orden de (20.103) es dos, necesitamos dos valores iniciales consecutivos. No los tenemos, pues sólo conocemos un valor inicial, $b_0 = 100$; para calcular b_2 debemos conocer también b_1,

$$b_2 = 4b_1 - 3b_0 = 4b_1 - 300,$$

de aquí que no tenga solución única.

IV. *Cálculo de las raíces características pertinentes*.

Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es

$$r^2 - 4r + 3,$$

que tiene dos raíces reales simples (con multiplicidad uno) distintas, $r_0 = 1$ y $r_1 = 3$.

V. *Obtención de las soluciones de las ED concernientes*.

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De acuerdo con el teorema 20.12 (pág. 1314 de esta edición) (teorema UNO), cualquier sucesión b_t que satisfaga (20.103) es de la forma

$$\begin{aligned} b_t &= \rho_0 \cdot 1^t + \rho_1 \cdot 3^t \\ &= \rho_0 + \rho_1 \cdot 3^t, \end{aligned}$$

para determinados números reales ρ_0 y ρ_1.

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

VI. *Obtención de la solución del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Así,

$$b_t = \rho_0 + \rho_1 \cdot 3^t \qquad (\rho_0, \rho_1 \in \mathbb{R})$$

es la solución general de (20.103), lo cual significa que existe un número infinito no numerable de sucesiones $\{b_t\}$ que son soluciones particulares de (20.103), cada una de ellas determinada por dos valores reales concretos de ρ_0 y ρ_1.

Sustituyendo el único valor inicial conocido,

$$\rho_1 = 100 - \rho_0,$$

de donde,

$$b_0 = 100 = \rho_0 + \rho_1 \cdot 3^0$$

y, por tanto, la solución general de (20.103) es

$$b_t = \rho_0 + (100 - \rho_0) \cdot 3^t \qquad (\rho_0 \in \mathbb{R}),$$

lo cual significa que existe un número infinito no numerable de sucesiones $\{b_t\}$ que son soluciones particulares de (20.103), cada una de ellas determinada por un valor real concreto de ρ_0. ■

Observación 20.5.28.— Por ejemplo, si $\rho_0 = 1$, entonces

$$\begin{aligned} b_n &= 1 + 99 \cdot 3^n \\ &= 9 \cdot (1 + 11 \cdot 3^n) - 8 \\ &= 9a_n - 8, \end{aligned}$$

donde la sucesión $a_n = 1 + 11 \cdot 3^n$ está catalogada como la sucesión A199114 en la OEIS[54].

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
a_n	12	34	100	298	892	2674	8020	24058	72172	216514	...
b_n	100	298	892	2674	8020	24058	72172	216514	649540	1948618	...

Observemos que $b_n = a_{n+2}$.

[54] *Vid*. https://oeis.org/A199114.

§ 20.5.3 Sistemas

Ejemplo 758

La relación evolutiva de dos comunidades digitales en estudio, D_0 y D_1, viene dada por: «Al final de cada día: el tamaño (número de individuos) de D_0 es igual al tamaño que D_0 tenía el día anterior más el tamaño que D_1 tenía el día anterior más el número de días que han transcurrido desde el inicio del estudio; el tamaño de D_1 es igual al tamaño que D_0 tenía el día anterior más tres individuos nuevos, menos el tamaño que D_1 tenía el día anterior». Supuesto que no existen factores externos que modifiquen sus crecimientos, se trata de que: 0., propongamos un sistema de ecuaciones en diferencias lineales que represente, según lo anterior, la relación entre los tamaños de las comunidades, dos días consecutivos, y 1., calculemos la solución general de dicho sistema.

[EFE 7.7.2017:8], [SEL 13:12].

Resolución.—

0. *Propuesta de un sistema de ecuaciones en diferencias lineales (SED).*

   I. *Propuesta de una ecuación en diferencias (ED) o más (en este caso, un sistema).*

   Sean:

$$x_n \leftrightharpoons \text{ tamaño de } D_0 \text{ el día } n,$$
$$y_n \leftrightharpoons \text{ tamaño de } D_1 \text{ el día } n.$$

   Del enunciado se deduce que un sistema de ecuaciones en diferencias lineales que representa la relación mencionada entre los tamaños de las comunidades dos días consecutivos es

$$x_n = x_{n-1} + y_{n-1} + n, \tag{20.104}$$
$$y_n = x_{n-1} + 3 - y_{n-1}. \tag{20.105}$$

1. *Resolución de dicho SED.*

La técnica es la misma que la ya vista en cuestiones anteriores de ecuación en diferencias interdependiente, esto es, extraer una de las sucesiones.

   I. *(Cont.) Propuesta de una ecuación en diferencias (ED).*

   De (20.104),

$$y_{n-1} = x_n - x_{n-1} - n, \tag{20.106}$$

sustituyendo en (20.105),

$$y_n = x_{n-1} + 3 - (x_n - x_{n-1} - n), \tag{20.107}$$

de (20.106),

$$y_n = x_{n+1} - x_n - (n+1), \tag{20.108}$$

igualando (20.108) y (20.107),

$$x_{n+1} - x_n - n - 1 = x_{n-1} + 3 - x_n + x_{n-1} + n,$$

simplificando,

$$x_{n+1} - 2x_{n-1} - 2n - 4 = 0,$$

que en forma estándar es

$$x_n - 2x_{n-2} = 2(n-1) + 4,$$

esto es,

$$x_n - 2x_{n-2} = 2n + 2, \tag{20.109}$$

la cual es una ecuación en diferencias lineal no homogénea con coeficientes constantes y de orden dos.

II. *Propuesta de un problema de valores iniciales (PVI).*

No procede (no se trata de un PVI porque no conocemos ninguna condición inicial).

III. *Demostración de que dicho PVI tiene solución única.*

No procede (por no tratarse de un PVI).

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). Dicha ecuación homogénea asociada a (20.109) es

$$x_n - 2x_{n-2} = 0,$$

cuyo polinomio característico,

$$r^2 - 2,$$

tiene dos raíces reales simples (con multiplicidad uno) distintas:

$$r_0 = -\sqrt{2},$$
$$r_1 = \sqrt{2}.$$

V. *Obtención de las soluciones de las ED concernientes.*

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

Por tanto, la solución general de la homogénea asociada es

$$x_n^{(h)} = c_0 \cdot (-\sqrt{2})^n + c_1 \cdot (\sqrt{2})^n (c_0, c_1 \in \mathbb{R}).$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

El término independiente, no homogéneo,

$$F(n) = 2n + 2,$$

es un polinomio que reescribimos como

$$F(n) = (2n + 2) \cdot 1^n,$$

de manera que en el teorema SEIS, $b_1 = 2$, $b_0 = 2$ y $s = 1$, y como 1 no es raíz característica, entonces, según dicho teorema, una solución de la no homogénea es

$$(p_1 n + p_0) \cdot 1^n,$$

esto es,

$$p_1 n + p_0.$$

Sustituyendo en la no homogénea (20.109),

$$(p_1 n + p_0) - 2 \cdot ((p_1(n-2) + p_0)) = 2n + 2,$$

de donde, simplificando y reordenando convenientemente, queda

$$-p_1 n + (4p_1 - p_0) = 2n + 2,$$

y ahora, por definición de igualdad de polinomios, deducimos que

$$p_0 = -10,$$
$$p_1 = -2,$$

por lo que una solución particular de la no homogénea es

$$x_n^{(p)} = -2n - 10.$$

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

Tenemos entonces que la solución general de la no homogénea es (cf. teorema CINCO):

$$x_n = x_n^{(h)} + x_n^{(p)}$$

$$= c_0 \cdot (-\sqrt{2})^n + c_1 \cdot (\sqrt{2})^n - 2n - 10 (c_0, c_1 \in \mathbb{R}). \tag{20.110}$$

Lo único que falta es calcular y_n.

Sustituyendo (20.110) en (20.108),

$$\begin{aligned} y_n &= x_{n+1} - x_n - (n+1) \\ &= (c_0 \cdot (-\sqrt{2})^{n+1} + c_1 \cdot (\sqrt{2})^{n+1} - 2(n+1) - 10) \\ &\quad - (c_0 \cdot (-\sqrt{2})^n + c_1 \cdot (\sqrt{2})^n - 2n - 10) - (n+1) \\ &= \ldots \\ &= -(\sqrt{2})^n \cdot ((1+\sqrt{2}) \cdot (-1)^n \cdot c_0 - \sqrt{2} \cdot c_1 + c_1) - n - 3 \qquad (c_0, c_1 \in \mathbb{R}). \end{aligned}$$

Así,

$$\begin{aligned} x_n &= c_0 \cdot (-\sqrt{2})^n + c_1 \cdot (\sqrt{2})^n - 2n - 10, \\ y_n &= -(\sqrt{2})^n \cdot ((1+\sqrt{2}) \cdot (-1)^n \cdot c_0 - \sqrt{2} \cdot c_1 + c_1) - n - 3 \qquad (c_0, c_1 \in \mathbb{R}), \end{aligned}$$

es la solución general del sistema de ecuaciones en diferencias lineales

$$\{x_n = x_{n-1} + y_{n-1} + n, y_n = x_{n-1} + 3 - y_{n-1}\},$$

lo cual significa que existe un número infinito no numerable de parejas de sucesiones $(\{x_n\}, \{y_n\})$ que son soluciones particulares de dicho sistema.

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

No procede, pues según el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), al ser de orden dos, debiésemos conocer dos valores iniciales consecutivos para poder obtener la solución única, pero no conocemos ninguno. ■

Ejemplo 759

Sean x_t e y_t los números totales de programas maliciosos pertenecientes a dos tipos, en la hora t, que coexisten en una cierta red de área extensa sometida a control horario de evolución de la malignidad programada en número de programas maliciosos. Supongamos que las poblaciones iniciales eran $x_0 = 3$ e $y_0 = 7$ y que la evolución de la coexistencia sigue la regla: cada hora, el crecimiento de la malignidad programada de tipo x es la suma del triple del crecimiento de x en la hora anterior y del crecimiento de y también en la hora anterior más siete nuevos programas maliciosos (que son clasificados como de tipo x), y también cada hora, el crecimiento de la malignidad programada de tipo y es el resultado de restar el crecimiento de x en la hora anterior del crecimiento de y en la hora anterior, más tres nuevos programas maliciosos (que son clasificados como de tipo y). Debemos: 0., proponer un sistema de ecuaciones en diferencias lineales que represente la evolución de la malignidad programada, y 1., resolver dicho sistema.

Resolución.— Analicemos la evolución del mal programado en función del crecimiento del mismo (el enunciado no especifica que sea en función de las poblaciones y así es más sencillo al disminuir en una unidad de tiempo el orden de la recurrencia).

0. *Propuesta de un sistema de ecuaciones en diferencias lineales (SED).*

   1. *Propuesta de una ecuación en diferencias (ED) o más (en este caso, un sistema).*

      Denotemos por X_t e Y_t los crecimientos desde la hora t a la hora $t+1$, o sea, $X_t = x(t+1) - x(t)$ e $Y_t = y(t+1) - y(t)$. El sistema de ecuaciones en diferencias lineales correspondiente a la situación que se plantea es

$$X_{t+1} = 3X_t + Y_t + 7, \tag{20.111}$$
$$Y_{t+1} = Y_t - X_t + 3. \tag{20.112}$$

1. *Resolución de dicho SED.*

   Seguimos aplicando la misma estrategia basada en la extracción de una de las sucesiones.

   1. *(Cont.) Propuesta de una ecuación en diferencias (ED).*

      De la primera ecuación,

$$Y_t = X_{t+1} - 3X_t - 7, \tag{20.113}$$

      de donde,

$$X_{t+2} = 3X_{t+1} + Y_{t+1} + 7. \tag{20.114}$$

Sustituyendo (20.112) en (20.114),

$$X_{t+2} = 3X_{t+1} + Y_t - X_t + 3 + 7.$$

Sustituyendo (20.113) en ésta, simplificando, agrupando y ordenando, obtenemos la ecuación en diferencias lineal no homogénea con coeficientes constantes y con función constante en el segundo miembro de la igualdad,

$$X_{t+2} - 4X_{t+1} + 4X_t = 3.$$

II. *Propuesta de un problema de valores iniciales (PVI).*

No procede en este momento (*vid. infra* VI [Paso V de ARED5]).

III. *Demostración de que dicho PVI tiene solución única.*

No procede en este momento (*vid. infra* VI [Paso V de ARED5]).

IV. *Cálculo de las raíces características pertinentes.*

Se trata de las raíces características de la homogénea asociada (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es $P(X) = X^2 - 4X + 4$, es decir, $P(X) = (X-2)^2$, que tiene como única raíz 2 con multiplicidad dos (raíz doble).

V. *Obtención de las soluciones de las ED concernientes.*

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

La solución general de la homogénea es

$$X_t = c_0 2^t + c_1 t 2^t \qquad (c_0, c_1 \in \mathbb{R})$$

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

Como la función del segundo miembro es constante, probamos con una constante cualquiera (número real) como posible solución particular, $k - 4k + 4k = 3$, de donde, $k = 3$, por lo que

$$X_t = 3$$

es una solución particular de la completa.

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

La solución general de la completa es

$$X_t = c_0 2^t + c_1 t 2^t + 3 \qquad (c_0, c_1 \in \mathbb{R}). \tag{20.115}$$

Solución general del SED.

Sustituyendo (20.115) en (20.111), simplificando, agrupando y ordenando, obtenemos

$$Y_t = (2c_1 - c_0)2^t - c_1 t 2^t - 13 \qquad (c_0, c_1 \in \mathbb{R}),$$

por lo que la solución general del SED es

$$\begin{aligned} X_t &= c_0 2^t + c_1 t 2^t + 3, \\ Y_t &= (2c_1 - c_0)2^t - c_1 t 2^t - 13, \end{aligned}$$

con $c_0, c_1 \in \mathbb{R}$.

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5) (ya para el SED).

Incorporación de las condiciones iniciales.

Sabemos que $x_0 = 3$ y $y_0 = 7$. Por tanto,

$$X_0 = x_1 - x_0 = x_1 - 3 = c_0 2^0 + c_1 \cdot 0 \cdot 2^0 + 3 = c_0 + 3,$$

de donde,

$$c_1 = x_1 - 6. \tag{20.116}$$

Por otro lado,

$$Y_0 = y_1 - y_0 = y_1 - 7 = (2c_1 - c_0)\, 2^0 - c_1 \cdot 0 \cdot 2^0 - 13 = 2c_1 - c_0 - 13,$$

en definitiva,

$$y_1 - 7 = 2c_1 - c_0 - 13. \tag{20.117}$$

Sustituyendo (20.116) en (20.117),

$$\begin{aligned} y_1 - 7 = 2c_1 - x_1 + 6 - 13 \to y_1 &= 2c_1 - x_1 \\ \to c_1 &= \frac{x_1 + y_1}{2}. \end{aligned}$$

Solución del caso planteado (evolución del mal programado en función del crecimiento del mismo).

$$\begin{aligned} X_t &= (x_1 - 6)\, 2^t + (x_1 + y_1)\, t 2^{t-1} + 3, \\ Y_t &= (y_1 + 6)\, 2^t - (x_1 + y_1)\, t 2^{t-1} - 13, \end{aligned}$$

donde x_1 e y_1 son las poblaciones de ambos tipos de programas maliciosos al finalizar la primera hora (datos no proporcionados en el enunciado). ∎

Ejemplo 760

Hallemos el número de secuencias de n términos con las letras a, b, c, d, tales que a nunca es adyacente a b.

[Cubit 163]. *Cfr.* Matoušek y Nešetřil [124]: ejercicio 12 (pág. 339).

Resolución.—

1. *Propuesta de una ecuación en diferencias (ED) o más.*

Sean:

$$u_n \leftrightharpoons \text{el número de secuencias que terminan con } a \text{ o } b,$$
$$v_n \leftrightharpoons \text{el número de secuencias que terminan con } c \text{ o } d,$$

con la condición de que a nunca es adyacente a b.

Observemos que la solución de la cuestión es $u_n + v_n$.

Ahora se trata de analizar la cuestión para poder aplicar la teoría de las ecuaciones en diferencias.

Veamos,

- por un lado, si la secuencia termina en a o b, el término anterior puede ser
  - c y el número de secuencias que terminan en c es v_{n-1}, o
  - d y el número de secuencias que terminan en d es v_{n-1},

  (si la secuencia termina en a, hemos de contar también el número de secuencias de longitud $n-1$ que terminan en a, y si la secuencia termina en b, hemos de contar también el número de secuencias de longitud $n-1$ que terminan en b; la suma de ambos recuentos es u_{n-1}),

  entonces, por el principio de la adición [¡esto requiere justificación! ✍],

$$u_n = u_{n-1} + 2v_{n-1};$$

- por otro lado, si la secuencia termina en c o d, el término anterior puede ser
  - c y el número de secuencias que terminan en c es v_{n-1}, o
  - d y el número de secuencias que terminan en d es v_{n-1}, o
  - a y el número de secuencias que terminan en a es u_{n-1}, o

- b y el número de secuencias que terminan en b es u_{n-1},

entonces, por el principio de la adición [¡esto requiere justificación! ✍],

$$v_n = 2v_{n-1} + 2u_{n-1}.$$

Este razonamiento ha sido regresivo («hacia atrás»); es muy recomendable que pensemos tranquilamente también en un razonamiento progresivo («hacia adelante)», esto es, construyendo la secuencia desde el primer término.

En cualquier caso, tenemos que resolver el sistema de ecuaciones en diferencias:

$$u_n = u_{n-1} + 2v_{n-1}, \tag{20.118}$$

$$v_n = 2v_{n-1} + 2u_{n-1}. \tag{20.119}$$

Veamos.

Vamos a extraer la ecuación en diferencias correspondiente a $\{u_n\}$ en la que solo participen términos de esta sucesión.

$$\begin{aligned} u_{n+1} &= u_n + 2v_n \qquad \text{[por (20.118)]}, \\ &= u_n + 2(2v_{n-1} + 2u_{n-1}) \qquad \text{[por (20.119)]}, \\ &= u_n + 4u_{n-1} + 4v_{n-1} \\ &= u_n + 4u_{n-1} + 4(u_n/2 - u_{n-1}/2) \qquad \text{[por (20.118)]}, \\ &= 3u_n + 2u_{n-1}, \end{aligned}$$

en resumen,

$$u_{n+1} = 3u_n + 2u_{n-1},$$

que en forma estándar es

$$u_n - 3u_{n-1} - 2u_{n-2} = 0 \qquad (n > 1).$$

II. *Propuesta de un problema de valores iniciales (PVI).*

Como es una ecuación en diferencias lineal de grado dos, por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), teniendo dos valores iniciales consecutivos, tenemos una solución particular.

Estos valores iniciales son:

$u_1 = 2$ (dos secuencias válidas: a, b),

$u_2 = 6$ (seis secuencias válidas: aa, ca, da, bb, cb, db).

El problema de valores iniciales de ecuaciones en diferencias que nos interesa es

$$\begin{aligned} u_n - 3u_{n-1} - 2u_{n-2} &= 0 \qquad (n > 1), \\ u_1 &= 2, \\ u_2 &= 6, \end{aligned} \tag{20.120}$$

III. *Demostración de que dicho PVI tiene solución única*.

Insistamos. Se trata de una ecuación en diferencias de orden dos, lineal, homogénea y de coeficientes constantes. Como sabemos por el teorema 20.4 (pág. 1302 de esta edición) (teorema CERO), un problema de valores iniciales de ecuaciones en diferencias, consistente en una ecuación de orden k y k condiciones iniciales consecutivas, tiene una única solución. Como el orden de (20.120) es dos, necesitamos dos valores iniciales consecutivos. Los tenemos: $u_1 = 2$ y $u_2 = 6$.

IV. *Cálculo de las raíces características pertinentes*. Se trata de las raíces características de la homogénea asociada (la propia ED de partida en este caso) (Paso I de ARED5 —*cfr. supra* § 20.4.5 (pág. 1328 de esta edición)—). El polinomio característico asociado a dicha ED es

$$r^2 - 3r - 2,$$

que tiene dos raíces reales simples (con multiplicidad uno) distintas, a saber,

$$\begin{aligned} r_0 &= \frac{3-\sqrt{17}}{2}, \\ r_1 &= \frac{3+\sqrt{17}}{2}. \end{aligned}$$

V. *Obtención de las soluciones de las ED concernientes*.

A. *Obtención de la solución general de la homogénea asociada* (Paso II de ARED5).

De lo anterior, de acuerdo con el teorema 20.12 (pág. 1314 de esta edición) (teorema UNO), cualquier sucesión $\{u_n\}$ que satisfaga (20.120) es de la forma:

$$u_n = \rho_0 \cdot \left(\frac{3-\sqrt{17}}{2}\right)^n + \rho_1 \cdot \left(\frac{3+\sqrt{17}}{2}\right)^n,$$

para determinados números reales ρ_0 y ρ_1.

Así,

$$u_n = \rho_0 \cdot \left(\frac{3-\sqrt{17}}{2}\right)^n + \rho_1 \cdot \left(\frac{3+\sqrt{17}}{2}\right)^n \qquad (\rho_0, \rho_1 \in \mathbb{R}), \tag{20.121}$$

es la solución general de (20.120), lo cual significa que existe un número infinito no numerable de sucesiones $\{u_n\}$ que son soluciones particulares de (20.120), cada una de ellas determinada por dos valores reales concretos de ρ_0 y ρ_1.

B. *Obtención de una solución particular de la completa* (Paso III de ARED5).

No procede (la ED es homogénea).

C. *Obtención de la solución general de la completa* (Paso IV de ARED5).

No procede (la ED es homogénea).

VI. *Obtención de la solución única del problema en estudio de valores iniciales de ecuaciones en diferencias* (Paso V de ARED5).

Sustituyendo los dos valores iniciales consecutivos en la solución general (20.121),

$$u_n = \rho_0 \cdot \left(\frac{3-\sqrt{17}}{2}\right)^n + \rho_1 \cdot \left(\frac{3+\sqrt{17}}{2}\right)^n \qquad (\rho_0, \rho_1 \in \mathbb{R}),$$

obtenemos el sistema de dos ecuaciones lineales con dos incógnitas ρ_0 y ρ_1,

$$(u_1 =)2 = \rho_0 \cdot \left(\frac{3-\sqrt{17}}{2}\right)^1 + \rho_1 \cdot \left(\frac{3+\sqrt{17}}{2}\right)^1,$$
$$(u_2 =)6 = \rho_0 \cdot \left(\frac{3-\sqrt{17}}{2}\right)^2 + \rho_1 \cdot \left(\frac{3+\sqrt{17}}{2}\right)^2,$$

cuya solución es

$$\rho_0 = -\frac{2}{\sqrt{17}},$$
$$\rho_1 = \frac{2}{\sqrt{17}},$$

esto es, una expresión explícita para $\{u_n\}$ es

$$u_n = -\frac{2}{\sqrt{17}}\left(\frac{3-\sqrt{17}}{2}\right)^n + \frac{2}{\sqrt{17}}\left(\frac{3+\sqrt{17}}{2}\right)^n,$$

o sea,

$$u_n = 2^{1-n}\frac{(3+\sqrt{17})^n - (3-\sqrt{17})^n}{\sqrt{17}}.$$

Entonces, por (20.118), para $n \geq 0$,

$$\begin{aligned} v_n &= \frac{u_{n+1} - u_n}{2} \\ &= \frac{1}{2}\left(2^{1-(n+1)}\frac{(3+\sqrt{17})^{n+1} - (3-\sqrt{17})^{n+1}}{\sqrt{17}} - 2^{1-(n+1)}\frac{(3+\sqrt{17})^{n+1} - (3-\sqrt{17})^{n+1}}{\sqrt{17}}\right) \\ &= 2^{-n-1}\frac{(\sqrt{17}-1)\cdot(3-\sqrt{17})^n + (\sqrt{17}+1)\cdot(3+\sqrt{17})^n}{\sqrt{17}}. \end{aligned}$$

La solución de la cuestión es la sucesión $\{u_n + v_n\}$, ésta es, para $n \geq 0$,

$$\begin{aligned} u_n + v_n &= 2^{1-n}\frac{(3+\sqrt{17})^n - (3-\sqrt{17})^n}{\sqrt{17}} \\ &\quad + 2^{-n-1}\frac{(\sqrt{17}-1)\cdot(3-\sqrt{17})^n + (\sqrt{17}+1)\cdot(3+\sqrt{17})^n}{\sqrt{17}} \\ &= 2^{-n-1}\frac{(\sqrt{17}-5)\cdot(3-\sqrt{17})^n + (\sqrt{17}+5)\cdot(3+\sqrt{17})^n}{\sqrt{17}}. \end{aligned}$$ ■

Actividad 20.11

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

Observación 20.5.29.— Las sucesiones $\{u_n\}$, $\{v_n\}$ y $\{u_n + v_n\}$ están catalogadas en la OEIS como las sucesiones A106434[55], A104934[56] y A055099[57], respectivamente, donde encontramos diversas fórmulas e interpretaciones. En particular, $\{u_n + v_n\}$ es la sucesión $\{s_n\}$ definida por el PVI

$$\begin{aligned} s_n - 3s_{n-1} - 2s_{n-2} &= 0 \qquad (n > 1), \\ u_0 &= 1, \\ u_1 &= 4. \end{aligned}$$

Enumerativamente:

n	0	1	2	3	4	5	6	7	8	9	...
u_n	0	2	6	22	78	278	990	3526	12558	44726	...
v_n	1	2	8	28	100	356	1268	4516	16084	57284	...
$u_n + v_n$	1	4	14	50	178	634	2258	8042	28642	102010	...

Observación 20.5.30.— Un sistema de ecuaciones en diferencias donde las sucesiones dependan las unas de las otras como el que ha aparecido en la cuestión anterior, también es conocido simplemente como *ecuación en diferencias interdependiente* o *ecuación en diferencias mutua*. Un concepto análogo es el de *recursión mutua*[58].

[55] *Vid*. https://oeis.org/A106434.
[56] *Vid*. https://oeis.org/A055099.
[57] *Vid*. https://oeis.org/A055099.
[58] *Cfr. v. gr.* https://es.wikipedia.org/wiki/Recursi%C3%B3n_mutua.

§ 20.6 En relación con la algoritmia

Una utilidad de las ecuaciones en diferencias se muestra en el cálculo de la *complejidad de un algoritmo*.

Otro tema es la *optimización*, en sus muchas variedades. Un ejemplo es la permanente búsqueda del algoritmo más rápido para multiplicar matrices. Si bien incluso es posible imaginar matrices continuas acotadas (el producto cartesiano $[0,1] \times [0,1]$) o continuas y no acotadas (el propio plano $\mathbb{R}^2$), de nuestro interés son las discretas, acotadas o no. Como hemos mencionado, en el caso de matrices discretas acotadas, ha sido de interés en estos años conseguir el algoritmo más rápido para calcular su producto.

§ 20.6.0 Resolución vía potencias de matrices

§ 20.7 Propuesta de más actividades

Actividad 20.12

Hallemos un problema de valores iniciales que defina la sucesión de cubos de números naturales.

Actividad 20.13

Supongamos un número ilimitado de coches y motos y un aparcadero con una fila de n espacios para aparcar motos grandes. Calculemos el número de formas de estacionarlos en dicha fila teniendo en cuenta que debe ocurrir a la vez que: I, cada moto ocupa un espacio y cada coche dos; II, las motos son idénticas entre sí y también los coches, y III, se tienen que ocupar todos los espacios.

[EFO 24.5.2018:7].

Actividad 20.14

En una simulación computacional predictiva se estudia una colectividad de entes futuros compatibles restringida a un área en la que se supone que salvo se diga algo en contra, no existen factores externos que afecten a su crecimiento. Supongamos una población inicial de doce entes, que ésta triplica su número en cada generación y que, además, cuatro nuevos entes se incorporan en cada generación procedentes del exterior. Calculemos el número de entes en una generación arbitraria n.

Actividad 20.15

Dado un conjunto de datos y una relación de orden total en él, se sabe de un algoritmo que el tiempo que necesita para ordenar n ítems depende del tiempo que necesita para ordenar $n-1$ más el tiempo necesario para situar al ítem enésimo en su lugar correcto en el orden. Supongamos que el tiempo requerido para el ítem enésimo es proporcional a n. Hallemos una fórmula explícita para calcular el tiempo que necesita para ordenar n ítems.

[SEL 12:1]. *Cfr.* Bradley [190]: ejercicio 5 (pág. 270).

Actividad 20.16

En un árbol de decisión determinado existen dos elecciones por nodo de elección. ¿Cuántas opciones disponibles hay tras n nodos de elección?

[SEL 12:2]. *Cfr.* Bradley [190]: ejercicio 17 (pág. 270).

Actividad 20.17

Se dibujan n rectas en un plano de forma que ni son paralelas dos a dos ni tres se intersecan en un mismo punto. ¿En cuántas regiones dividen al plano n de tales rectas?

[SEL 12:5]. *Cfr.* Bradley [190]: ejercicio 21 (pág. 271).

Actividad 20.18

Calculemos el número de palabras de n bits que no contienen tres unos consecutivos.

[SEL 12:6]. *Cfr.* Johnsonbaugh [158]: ejemplo 7.1.6 (pág. 330).

Actividad 20.19

Ésta se refiere a Tito y Samuel, que lanzan monedas no cargadas: si las monedas son ambas cara o ambas cruz, Tito gana; si una moneda tiene cara y la otra cruz, Samuel gana. Tito comienza con T monedas y Samuel comienza con S monedas. Calculemos la probabilidad p_n de que Tito gane todas las monedas de Samuel si Tito comienza con n monedas.

Esto tiene que ver con el problema de la ruina. Veamos, por ejemplo, en español, *El problema de la ruina del jugador*, de Jesús de la Cal Aguado [221], donde la sección cuarta es muy sugerente para la cuestión que nos ocupa.

[SEL 12:7]. *Cfr.* Johnsonbaugh [158]: ejercicio 35 (pág. 348).

Actividad 20.20

Dos preguntas:

0. ¿cuántas maneras existen de escribir el número entero positivo n como suma de unos y doses?;

1. ¿cuántas soluciones existen para la ecuación $x_1 + x_2 + \ldots + x_k = n$, con $x_i \in \{1, 2\}$, $i \in \{1, 2, \ldots, k\}$, $k \in \{1, 2, \ldots\}$?

[SEL 13:1]. *Cfr.* Matoušek y Nešetřil [124]: Otra consecuencia (pág. 335).

Actividad 20.21

(*Mini-Tetris*, III–VI). Consideremos un tablero rectangular de $2 \times n$ dividido en $2n$ cuadrados. Calculemos el número de maneras de cubrir exactamente, esto es, por completo y sin superposiciones, este tablero, con piezas de los siguientes tipos, estando permitido girar las piezas en ángulos que sean múltiplos de un ángulo recto. Hallémoslo en estos casos:

0. con sólo cuadrados 1×1 y 2×2;
1. con sólo cuadrados 1×1 y piezas en forma de ele (trominós L) 2×2 (piezas cuadradas 2×2 a las que les falta el cuadrado 1×1 superior derecho);
2. con sólo dominós 1×2 y trominós L 2×2;
3. con sólo cuadrados 2×2, dominós 1×2 y trominós L 2×2.

[SEL 13:2b]. *Cfr.* Matoušek y Nešetřil [124]: ejercicio 13 (pág. 339).

Con miras a su resolución.— Con respecto al apartado 0., observemos que esta cuestión es equivalente a la estudiada en el ejemplo 739 (pág. 1341 de esta edición) (del robot «caminante») —en efecto: la longitud n de la caminata es equivalente a la longitud n del tablero (supongámoslo «tumbado» por el lado de longitud n); comenzar con un paso de un metro equivale a empezar el cubrimiento con la configuración ⊟, quedando por cubrir un tablero $2 \times (n-1)$, y comenzar con un paso de dos metros equivale a empezar el cubrimiento con la configuración □, quedando por cubrir un tablero $2 \times (n-2)$; por todo esto, proponemos la ecuación en diferencias $a_n = a_{n-1} + a_{n-2}$, la cual, junto a los valores iniciales $a_1 = 1$ —sólo hay una forma, ⊟— y $a_2 = 2$ —hay dos formas: ⊞ y □—, conforman el problema de valores iniciales que hemos de resolver, cuya solución, como sabemos, es $a_n = F_{n+1}$.

Con respecto al apartado 1., las configuraciones iniciales válidas son ⊟⊟, ⌊, ⌋, ⌊□ y □⌋, por lo que proponemos la ecuación $a_n = a_{n-1} + b_{n-1} + b_{n-1} + a_{n-2} + a_{n-2}$; por otra parte, las configuraciones segunda y tercera dejan por cubrir un tablero $2 \times n$ con una esquina cuadrada 1×1 faltante; las configuraciones iniciales válidas para cualquiera de ellas son dos, para la primera, □ y ⌈, y para la segunda, □ y ⌉, por lo que proponemos la ecuación $b_{n-1} = a_{n-2} + a_{n-3}$; así, tenemos el sistema $\{a_n = a_{n-1} + b_{n-1} + b_{n-1} + a_{n-2} + a_{n-2}, b_{n-1} = a_{n-2} + a_{n-3}\}$, del cual, sustituyendo la segunda en la primera, obtenemos la ecuación en diferencias $a_n = a_{n-1} + 4a_{n-2} + 2a_{n-3}$, la cual, junto a los valores iniciales $a_0 = 1$, $a_1 = 1$ y $a_2 = 5$, conforman el problema de valores iniciales que hemos de resolver. Como el polinomio característico tiene una raíz real y dos complejas, esta cuestión sobresale del marco que acota estas notas, por lo que recurrimos, por ejemplo, a Wolfram|Alpha[59], con la petición `a(n) = a(n-1) + 4*a(n-2) + 2*a(n-3), a(0) = 1, a(1) = 1, a(2) = 5`, observando que la solución

[59] *Cfr.* https://www.wolframalpha.com/.

es la sucesión 1, 1, 5, 11, 33, 87, 241, 655, 1793, 4895, . . ., catalogada como la sucesión A127864 en la OEIS[60], donde su nombre es precisamente el cubrimiento con las piezas que aquí analizamos.

Con respecto al apartado 2., las configuraciones iniciales válidas son , , y , por lo que proponemos la ecuación $a_n = a_{n-1} + a_{n-2} + b_{n-1} + b_{n-1}$; por otra parte, las configuraciones segunda y tercera dejan por cubrir un tablero $2 \times n$ con una esquina cuadrada 1×1 faltante; las configuraciones iniciales válidas para cualquiera de ellas son dos, para la primera, y , y para la segunda, y , por lo que proponemos la ecuación $b_{n-1} = b_{n-2} + a_{n-3}$; así, tenemos el sistema $\{a_n = a_{n-1} + a_{n-2} + b_{n-1} + b_{n-1}, b_{n-1} = b_{n-2} + a_{n-3}\}$, del cual, sustituyendo la segunda en la primera, obtenemos la ecuación en diferencias $a_n = 2a_{n-1} + a_{n-3}$, la cual, junto a los valores iniciales $a_1 = 1$, $a_2 = 2$ y $a_3 = 5$, conforman el problema de valores iniciales que hemos de resolver. Como el polinomio característico tiene una raíz real y dos complejas, esta cuestión sobresale del marco que acota estas notas, por lo que recurrimos, por ejemplo, a Wolfram|Alpha[61], con la petición `a(n) - 2*a(n-1) - a(n-3) = 0, a(1) = 1, a(2) = 2, a(3) = 5`, observando que la solución es la sucesión 1, 2, 5, 11, 24, 53, 117, 258, 569, 1255, . . ., catalogada como la sucesión A052980 en la OEIS[62], con a(0) = 1, donde, en el tercer comentario, aparece su interpretación en términos de dominós y trominós L.

Con respecto al apartado 3., las configuraciones iniciales son , , , y , por lo que proponemos la ecuación $a_n = b_{n-1} + b_{n-1} + a_{n-2} + a_{n-2} + a_{n-1}$; por otra parte, como hemos visto en el apartado 2., $b_{n-1} = b_{n-2} + a_{n-3}$; así, tenemos el sistema $\{a_n = 2b_{n-1} + 2a_{n-2} + a_{n-1}, b_{n-1} = b_{n-2} + a_{n-3}\}$, del cual, despejando de la primera, $2b_{n-1} = a_n - a_{n-1} - 2a_{n-2}$ y $2b_{n-2} = a_{n-1} - a_{n-2} - 2a_{n-3}$, de donde, sustituyendo b_{n-1} y b_{n-2} en $b_{n-1} = b_{n-2} + a_{n-3}$, obtenemos la ecuación en diferencias $a_n - 2a_{n-1} - a_{n-2} = 0$, la cual, junto a los valores iniciales consecutivos $a_1 = 1$ y $a_2 = 4$, conforman el problema de valores iniciales que hemos de resolver. La solución es la sucesión 1, 4, 9, 22, 53, 128, 309, 746, 1801, 4348, . . ., catalogada como la sucesión A048654 en la OEIS[63].

Observación 20.7.0.— Los trominós[64], al igual que los dominós[65] y los monominós (los cuadrados[66]) son un caso particular de poliminós[67].

Actividad 20.22

Consideremos una red poligonal de n nodos (vértices), $n \geq 2$, y sea $N(n)$ el número de aristas (lados + diagonales). Dicho esto:

0. obtengamos razonadamente una ecuación en diferencias para $N(n)$;
1. calculemos su solución general;
2. calculemos la solución particular correspondiente a esta situación.

[EFE 7.7.2017:7], [SEL 13:4].

---

[60] https://oeis.org/A127864.
[61] *Cfr.* https://www.wolframalpha.com/.
[62] https://oeis.org/A052980.
[63] https://oeis.org/A048654.
[64] *Vid. v. gr.* https://en.wikipedia.org/wiki/Tromino.
[65] *Vid. v. gr.* https://en.wikipedia.org/wiki/Domino_(mathematics).
[66] *Vid. v. gr.* https://en.wikipedia.org/wiki/Square.
[67] *Vid. v. gr.* https://en.wikipedia.org/wiki/Polyomino.

Actividad 20.23

(Problema de la persona viajante de comercio) Imaginemos que somos una persona viajante de comercio y consideremos n ciudades, incluida la nuestra propia, que debemos visitar. Supongamos también que conocemos todas las distancias entre dos cualesquiera de ellas. Comenzando en nuestra ciudad, hemos de decidir el orden en que visitamos todas las ciudades, de manera que sea mínima la distancia (o el tiempo) total de llegar a todas y volver a nuestra ciudad. La forma más obvia de resolverlo es con una técnica exhaustiva: 0.º, hacemos una lista con todas las rutas posibles; 1.º, calculamos la longitud de cada una, y 2.º, seleccionamos la ruta más corta. ¿Cuántas rutas debe examinar este algoritmo exhaustivo?

[SEL 13:5]. *Cfr.* Bradley [190]: ejercicio 10.36 (págs. 2–3 y 263–264).

Actividad 20.24

Sea P_n el número de particiones de un conjunto de n elementos. Demostremos que la sucesión $P_0, P_1, \ldots$, satisface la ecuación en diferencias $P_n = \sum_{k=0}^{n-1} \binom{n-1}{k} P_k$.

[SEL 13:8]. *Cfr.* Johnsonbaugh [158]: ejercicio 4 del *Self-Test* (pág. 371).

Actividad 20.25

Si α es una palabra de bits, sea $C(\alpha)$ el número máximo de ceros consecutivos en α. [*Ejemplos*: $C(10010) = 2$, $C(00110001) = 3$]. Sea S_n el número de palabras α de n bits con $C(\alpha) \leq 2$. Hallemos S_n.

[SEL 13:10]. *Cfr.* Johnsonbaugh [158]: ejercicio 61 (pág. 337).

Actividad 20.26

Notemos por $C_b(n)$ el número de palabras de longitud $n \geq 1$, en base b, que no contienen dos dígitos consecutivos iguales. Dicho esto:

0. obtengamos razonadamente una ecuación en diferencias lineal para $C_2(n)$, calculemos su solución general y la particular correspondiente a esta situación;
1. Hagamos lo mismo para $b = 3$, esto es, obtengamos razonadamente una ecuación en diferencias lineal para $C_3(n)$, calculemos su solución general y la particular correspondiente a esta situación;
2. ¿es extensible nuestro razonamiento al caso de una base $b \geq 3$? Justifiquemos nuestra respuesta.

[SEL 13:11].

Actividad 20.27

Una ONG sobre medioambiente y conservación de la biodiversidad ha realizado un estudio sobre la evolución de dos especies, E_0 y E_1, que comparten un mismo territorio sometido a presión humana. El texto del informe incluye la siguiente descripción (los datos que se mencionan se recogen al finalizar cada año):

«Cada año, de la especie E_0 nacen tantos como individuos, de esa especie, había el año anterior y fallecen tantos como el doble de individuos de la especie E_1 había el año anterior, mientras que de la especie E_1, fallecen tantos como el doble de individuos, de esa especie, había el año anterior y nacen tantos como individuos había el año anterior de la especie E_0».

Supuesto que no hay inmigraciones ni emigraciones ni influyen factores externos que modifiquen sus crecimientos, se trata de que:

0. escribamos un sistema de ecuaciones en diferencias lineales que represente, según lo anterior, la relación entre los tamaños de las poblaciones, dos años consecutivos;
1. calculemos la solución general de dicho sistema;
2. interpretemos dicha solución, informando del comportamiento en el muy largo plazo de ambas poblaciones.

[EFE 1.6.2017:8], [SEL 13:13].

Actividad 20.28

Se ha hecho un estudio para determinar la satisfacción de la clientela de dos compañías de servicios, A y B, con dos supuestos: todas las personas del estudio han contratado los servicios de A o de B y cualquiera de ellas es libre de cambiar de compañía cada mes sin cargos. Ha resultado que $1/3$ de la clientela de A se sienten satisfechas con A y volverán a contratar a A el mes siguiente pero $2/3$ de la clientela de A están insatisfechas con los servicios que proporciona A y cambiarán a la compañía B, y que la mitad de la clientela de B confían en B y se mantendrán fieles a ella, mientras que la otra mitad cambiarán de compañía. Inicialmente (esto es, en la fecha de inicio del experimento), $1/3$ de la población total está con la compañía A y $2/3$ con B.

Siendo a_n y b_n las poblaciones (número de clientes) en el mes n de las firmas A y B, respectivamente, nos preguntamos:

0. ¿cuál es la distribución de la clientela transcurridos n meses?;
1. ¿qué ocurrirá en el muy largo plazo con dicha distribución de clientes?

[SEL 13:14].

§ 20.8 Muestra de ejemplos finales

Ejemplo 761

En § 19.3.5 (pág. 1215 de esta edición) hemos interpretado las soluciones enteras no negativas de $x_1+x_2+\cdots+x_n = k$ ($k, n \in \mathbb{Z}^+$) en el contexto de la selección de muestras, la distribución de objetos en recipientes, la partición de un multiconjunto en submulticonjuntos y la descomposición de un entero positivo en sumandos enteros no negativos. Aquí nos proponemos lo siguiente: si s_k representa el número de soluciones enteras no negativas de $x_1 + x_2 + \cdots + x_n = k$, hallar una ecuación en diferencias para s_k (n fijo) y encontrar finalmente una expresión explícita tan simple como sea posible para s_k.

[EFO 12.6.2020:4a (p.h.e.c.)].

Resolución.— De la ecuación diofántica $x_1 + x_2 + \cdots + x_n = k$, sabemos[68] que el número de soluciones enteras no negativas es $CR(n, k)$, esto es, $C(k + n - 1, n - 1)$, reescribible como $C(k + n - 1, k)$; en otras palabras, $s_k = C(k + n - 1, k)$.

Vía 0.

La propia definición de número combinatorio en función de los factoriales de números nos proporciona una definición recurrente de número combinatorio, a saber,

$$\begin{aligned}\binom{n}{k} &= \frac{n!}{k!\cdot(n-k)!}\\ &= \frac{n\cdot(n-1)!}{k\cdot(k-1)!\cdot(n-k)!}\\ &= \frac{n}{k}\cdot\frac{(n-1)!}{(k-1)!\cdot(n-k)!}\\ &= \frac{n}{k}\binom{n-1}{k-1},\end{aligned}$$

válida $\forall n, k \in \mathbb{N}, 1 \leq k \leq n$.

Para el caso que nos ocupa, $\forall n, k + n - 1 \in \mathbb{N}, 1 \leq k \leq k + n - 1$,

$$\begin{aligned}s_k = \binom{k+n-1}{k} &= \frac{k+n-1}{k}\binom{k+n-1-1}{k-1}\\ &= \frac{k+n-1}{k}\binom{(k-1)+n-1}{k-1},\end{aligned}$$

[68] *Cfr. supra* teorema 19.43 (pág. 1186 de esta edición), para $m = 0$.

y, por tanto,

$$s_k = \frac{k+n-1}{k} \cdot s_{k-1} \tag{20.122}$$

La ecuación (20.122) es una ecuación en diferencias lineal homogénea con coeficientes no constantes, de orden 1, para s_k (n fijo).

Aunque sea de coeficientes no constantes, tratemos de encontrar una fórmula explícita, por ejemplo, mediante sustitución hacia adelante.

Fase I. *Expansión*.

$$\begin{aligned}
s_2 &= \frac{2+n-1}{2} \cdot s_1 = \frac{n+1}{2} \cdot s_1 \\
s_3 &= \frac{3+n-1}{3} \cdot s_2 = \frac{3+n-1}{3} \cdot \frac{2+n-1}{2} \cdot s_1 = \frac{n+2}{3} \cdot \frac{n+1}{2} \cdot s_1 \\
s_4 &= \frac{4+n-1}{4} \cdot s_3 = \frac{4+n-1}{4} \cdot \frac{3+n-1}{3} \cdot \frac{2+n-1}{2} \cdot s_1 = \frac{n+3}{4} \cdot \frac{n+2}{3} \cdot \frac{n+1}{2} \cdot s_1 \\
&\vdots
\end{aligned}$$

Fase II. *Intuición*.

Intuimos que

$$s_k = \frac{k+n-1}{k} \cdot \frac{k+n-2}{k-1} \cdot \ldots \cdot \frac{n+2}{3} \cdot \frac{n+1}{2} \cdot s_1,$$

esto es,

$$\begin{aligned}
s_k &= s_1 \cdot \frac{1}{k!} \cdot (k+n-1) \cdot (k+n-2) \cdot \ldots \cdot (n+2) \cdot (n+1) \\
&= s_1 \cdot \frac{1}{k!} \cdot \frac{(k+n-1)!}{n!} \\
&= s_1 \cdot \frac{(k+n-1)!}{k! \cdot n \cdot (n-1)!} \\
&= s_1 \cdot \frac{1}{n} \cdot \frac{(k+n-1)!}{k! \cdot (n-1)!} \\
&= s_1 \cdot \frac{1}{n} \cdot \binom{k+n-1}{k},
\end{aligned}$$

siendo $s_1 \in \mathbb{R}$.

Fase III. *Demostración*.

Por ejemplo, mediante inducción débil. Para ello, apliquemos el teorema de inducción débil[69].

Caso base (ID_0).— Para $n = 1$, según lo que hemos intuido, $s_1 = s_1 \cdot \frac{1}{n} \cdot \binom{1+n-1}{1}$, lo cual es cierto; en otras palabras, se satisface $P(1)$.

[69] *Vid*. teorema 16.0 (pág. 805 de esta edición).

Paso inductivo (ID_1).— Supongamos $P(k)$ y demostremos $P(k+1)$, esto es, supongamos que $s_k = s_1 \cdot \frac{1}{n} \cdot \binom{k+n-1}{k}$ (*hipótesis inductiva*) y demostremos que $s_{k+1} = s_1 \cdot \frac{1}{n} \cdot \binom{(k+1)+n-1}{k+1}$, es decir, que $s_{k+1} = s_1 \cdot \frac{1}{n} \cdot \binom{k+n}{k+1}$ (*tesis inductiva*); en efecto, según (20.122), $s_{k+1} = \frac{(k+1)+n-1}{k+1} \cdot s_{(k+1)-1}$, esto es, $s_{k+1} = \frac{k+n}{k+1} \cdot s_k$ y por la hipótesis inductiva, $s_{k+1} = \frac{k+n}{k+1} \cdot s_1 \cdot \frac{1}{n} \cdot \binom{k+n-1}{k}$, esto es,

$$\begin{aligned} s_{k+1} &= s_1 \cdot \frac{1}{n} \cdot \frac{k+n}{k+1} \cdot \frac{(k+n-1)!}{k! \cdot (n-1)!} \\ &= s_1 \cdot \frac{1}{n} \cdot \frac{(k+n)!}{(k+1)! \cdot (n-1)!} \\ &= s_1 \cdot \frac{1}{n} \cdot \binom{k+n}{k+1}; \end{aligned}$$

en otras palabras, se satisface $P(k+1)$.

Conclusión ($ID_0 \wedge ID_1$).— Como se satisfacen el caso base y el paso inductivo, entonces, del teorema de inducción débil[70] se sigue lo buscado, a saber, que $s_k = s_1 \cdot \frac{1}{n} \cdot \binom{k+n-1}{k}$ es cierto para todo $k \in \mathbb{Z}^+$.

En definitiva, hemos encontrado y demostrado, mediante sustitución hacia adelante, que la expresión explícita de la solución general de (20.122), es

$$s_k = c \cdot \frac{1}{n} \cdot \binom{k+n-1}{k} \quad (c \in \mathbb{R}). \tag{20.123}$$

Hallemos finalmente la expresión explícita de la solución particular del caso que nos ocupa. Por ser de orden 1 la ecuación (20.122), para asegurar que tiene solución necesitamos una condición inicial[71]. Notemos que $s_1 = n$ ya que el número de soluciones enteras no negativas de $x_1 + x_2 + \cdots + x_n = 1$ es n, pues las soluciones son $(1,0,0,0,\ldots,0,0)$, $(0,1,0,0,\ldots,0,0)$, $(0,0,1,0,\ldots,0,0)$, ..., $(0,0,0,0,\ldots,1,0)$, $(0,0,0,0,\ldots,0,1)$ (es decir, tantas como veces el 1 es una única vez cada sumando x_i, esto es, n).

De este modo, sustituyendo el valor inicial en la solución general (20.123), obtenemos la ecuación lineal con una incógnita

$$\begin{aligned} s_1 = n &= c \cdot \frac{1}{n} \cdot \binom{1+n-1}{1} \\ &= c \cdot \frac{1}{n} \cdot n, \end{aligned}$$

70 *Vid.* teorema 16.0 (pág. 805 de esta edición).

71 *Vid. supra* teorema 20.4 (pág. 1302 de esta edición) (teorema CERO).

cuya solución es

$$c = n,$$

por lo que sustituyendo en (20.123), obtenemos que la expresión explícita de la solución particular del caso en estudio es

$$s_k = n \cdot \frac{1}{n} \cdot \binom{k+n-1}{k},$$

esto es,

$$s_k = \binom{k+n-1}{k}.$$

Solución,— Dado $n \in \mathbb{Z}^+$, se tiene:

0.°, una ecuación en diferencias para s_k es $s_k = \dfrac{k+n-1}{k} \cdot s_{k-1}$;

1.°, la solución explícita de esta ecuación es $s_k = c \cdot \dfrac{1}{n} \cdot \dbinom{k+n-1}{k}$ $(c \in \mathbb{R})$, y

2.°, la solución explícita del correspondiente problema de valores para el caso en estudio, correspondiente a $s_1 = n$, es $s_k = \dbinom{k+n-1}{k}$. □

Vía 1.

Investiguemos los primeros valores de n:

- sea $n = 2$, esto es, $x_1 + x_2 = k$; como $k > 0$ $(k \in \mathbb{Z}^+)$, entonces, $x_1 > 0$ o $x_2 > 0$; entonces, por un lado, una solución con $x_1 > 0$ significa que $(x_1 - 1, x_2)$ es solución de $x_1 + x_2 = k - 1$, por lo que hay s_{k-1} soluciones de esta última; por otro, por un razonamiento similar, hay s_{k-1} soluciones para $x_2 > 0$, y, por otro, hay $s_{k-(1+1)}$ soluciones para $x_1 > 0$ y $x_2 > 0$;

  entonces, por el principio de inclusión-exclusión (PIE)[72], siendo S_1 el conjunto de soluciones (x_1, x_2) de $x_1 + x_2 = k$ tales que $x_1 > 0$, S_2 el conjunto de soluciones (x_1, x_2) de $x_1 + x_2 = k$ tales que $x_2 > 0$ y $S_1 \cap S_2$ el conjunto de soluciones (x_1, x_2) de $x_1 + x_2 = k$ tales que $x_1 > 0$ y $x_2 > 0$, conjuntos S_1, S_2 y $S_1 \cap S_2$ cuyos cardinales respectivos son s_{k-1}, s_{k-1} y $s_{k-(1+1)}$—, se tiene que una ecuación en diferencias para s_k es

$$s_k = s_{k-1} + s_{k-1} - s_{k-(1+1)},$$

  esto es,

$$s_k = 2s_{k-1} - s_{k-2},$$

  en forma estándar,

$$s_k - 2s_{k-1} + s_{k-2} = 0, \tag{20.124}$$

[72] *Vid. supra* teorema 19.27 (pág. 1147 de esta edición).

siendo una expresión explícita para su solución general $^{(*)}$,

$$s_k = c_2 k + c_1, \tag{20.125}$$

con $c_1, c_2 \in \mathbb{R}$;

por ejemplo, calculemos s_3: por un lado, $s_1 = 2$ —las dos soluciones enteras no negativas de $x_1 + x_2 = 1$, a saber, $(0, 1)$ y $(1, 0)$—; por otro, $s_2 = 3$ —las 3 soluciones enteras no negativas de $x_1 + x_2 = 2$, a saber, $(0, 2)$, $(1, 1)$ y $(2, 0)$—; entonces, sustituyendo en (20.125):

$$s_1 = 2 = c_2 \cdot 1 + c_1,$$
$$s_2 = 3 = c_2 \cdot 2 + c_1,$$

de donde $c_1 = 1$ y $c_2 = 1$, por lo que $s_3 = 1 \cdot 3 + 1 = 4$ —las cuatro soluciones enteras no negativas de $x_1 + x_2 = 3$, a saber, $(0, 3)$, $(1, 2)$, $(2, 1)$ y $(3, 0)$—, lo cual coincide con lo conocido, $s_3 = C(3 + 2 - 1, 2 - 1) = C(4, 1) = 4$;

por otra parte, es posible calcular una expresión explícita de la solución particular de la situación en estudio, para $n = 2$, simplemente sustituyendo los valores $c_1 = 1$ y $c_2 = 1$ en (20.125), esto es,

$$s_k = 1 \cdot k + 1,$$

esto es,

$$\begin{aligned} s_k &= k + 1 \\ &= \binom{k+1}{1}, \end{aligned}$$

es decir, para $n = 2$,

$$s_k = \binom{k+2-1}{2-1};$$

- de manera similar, para $n = 3$, esto es, para la ecuación $x_1 + x_2 + x_3 = k$,

$$s_k = s_{k-1} + s_{k-1} + s_{k-1} - s_{k-(1+1)} - s_{k-(1+1)} - s_{k-(1+1)} + s_{k-(1+1+1)},$$

esto es,

$$s_k = 3s_{k-1} - 3s_{k-2} + s_{k-3},$$

en forma estándar,

$$s_k - 3s_{k-1} + 3s_{k-2} - s_{k-3} = 0, \tag{20.126}$$

y una expresión explícita para su solución general es $^{(*)}$

$$s_k = c_3 k^2 + c_2 k + c_1, \tag{20.127}$$

con $c_1, c_2, c_3 \in \mathbb{R}$;

ahora, para calcular una expresión explícita de la solución particular de la situación en estudio necesitamos conocer s_1, s_2 y s_3. Veamos, por un lado, $s_1 = 3$, ya que $(0, 0, 1)$, $(0, 1, 0)$ y $(1, 0, 0)$ son las soluciones enteras no negativas de $x_1 + x_2 + x_3 = 1$; por otro, $s_2 = 6$, ya que $(0, 0, 2)$, $(0, 2, 0)$, $(2, 0, 0)$, $(0, 1, 1)$, $(1, 0, 1)$ y $(1, 1, 0)$ son las soluciones enteras no negativas de $x_1 + x_2 + x_3 = 2$, y por otro, $s_3 = 10$, ya que $(0, 0, 3)$, $(0, 3, 0)$, $(3, 0, 0)$, $(0, 2, 1)$, $(2, 0, 1)$, $(2, 1, 0)$, $(0, 1, 2)$, $(1, 0, 2)$, $(1, 2, 0)$ y $(1, 1, 1)$ son las soluciones enteras no negativas de $x_1 + x_2 + x_3 = 3$;

finalmente, sustituyendo en (20.127),

$$\begin{aligned} s_1 = 3 &= c_3 \cdot 1^2 + c_2 \cdot 1 + c_1, \\ s_2 = 6 &= c_3 \cdot 2^2 + c_2 \cdot 2 + c_1, \\ s_3 = 10 &= c_3 \cdot 3^2 + c_2 \cdot 3 + c_1, \end{aligned}$$

de donde $c_1 = 1$, $c_2 = 3/2$ y $c_3 = 1/2$, por lo que una expresión explícita de la solución particular de la situación en estudio, para $n = 3$, sustituyendo estos valores en (20.127), es

$$\begin{aligned} s_k &= \frac{1}{2}k^2 + \frac{3}{2}k + 1 \\ &= \frac{k^2 + 3k + 2}{2} \\ &= \frac{(k+2) \cdot (k+1)}{2} \\ &= \frac{(k+2) \cdot (k+1) \cdot k!}{2 \cdot k!} \\ &= \binom{k+2}{2}, \end{aligned}$$

es decir, para $n = 3$,

$$s_k = \binom{k+3-1}{3-1};$$

- igualmente, para $n = 4$, demostraríamos que una ecuación en diferencias para s_k, en forma estándar, es

$$s_k - 4s_{k-1} + 6s_{k-2} - 4s_{k-3} + s_{k-4} = 0,$$

de la que una expresión explícita para su solución general es

$$s_k = c_4k^3 + c_3k^2 + c_2k + c_1,$$

con $c_1, c_2, c_3, c_4 \in \mathbb{R}$, y que una expresión explícita de la solución particular de la situación en estudio es

$$s_k = \binom{k+4-1}{4-1};$$

- análogamente, para $n = 5$, demostraríamos que una ecuación en diferencias para s_k, en forma estándar, es
$$s_k - 5s_{k-1} + 10s_{k-2} - 10s_{k-3} + 5s_{k-4} - s_{k-5} = 0,$$
de la que una expresión explícita para su solución general es
$$s_k = c_5k^4 + c_4k^3 + c_3k^2 + c_2k + c_1,$$
con $c_1, c_2, c_3, c_4, c_5 \in \mathbb{R}$, y que una expresión explícita de la solución particular de la situación en estudio es
$$s_k = \binom{k+5-1}{5-1};$$
- similarmente, para $n = 6$, demostraríamos que una ecuación en diferencias para s_k, en forma estándar, es
$$s_k - 6s_{k-1} + 15s_{k-2} - 20s_{k-3} + 15s_{k-4} - 6s_{k-5} + s_{k-6} = 0,$$
de la que una expresión explícita para su solución general es
$$s_k = c_6k^5 + c_5k^4 + c_4k^3 + c_3k^2 + c_2k + c_1,$$
con $c_1, c_2, c_3, c_4, c_5, c_6 \in \mathbb{R}$, y que una expresión explícita de la solución particular de la situación en estudio es
$$s_k = \binom{k+6-1}{6-1};$$
- etc.

Observamos cómo los coeficientes, en valor absoluto, para los diferentes valores de n, son los números de la fila n del triángulo de Pascal[73], lo cual no tiene nada de extraño, ya que estamos aplicando PIE en todos los casos y ocurre como en la versión probabilística de PIE[74], a saber, que todos los cardinales de las intersecciones del mismo número de conjuntos son iguales.

Solución.— Razonando similarmente para un n arbitrario, mediante el principio de inclusión-exclusión, siendo S_j el conjunto de soluciones $(x_1, x_2, \ldots, x_n)$ de $x_1 + x_2 + \cdots + x_n = k$ tales que $x_j > 0$ ($j \in \{1, 2, \ldots, n\}$), cuyos cardinales son $|S_j| = s_{k-1}$, $S_i \cap S_j$ (las intersecciones dos a dos) el conjunto de soluciones $(x_1, x_2, \ldots, x_n)$ de $x_1 + x_2 + \cdots + x_n = k$ tales que $x_i > 0$ y $x_j > 0$ ($i, j \in \{1, 2, \ldots, n\}$, $i \neq j$), cuyos cardinales son $|S_i \cap S_j| = s_{k-2}$, y así sucesivamente, hasta $S_1 \cap S_2 \cap \ldots \cap S_n$, el conjunto de soluciones $(x_1, x_2, \ldots, x_n)$ de $x_1 + x_2 + \cdots + x_n = k$ tales que $x_1 > 0$, $x_2 > 0$, …, $x_{n-1} > 0$ y $x_n > 0$, cuyo cardinal es s_{k-n}—, demostraríamos que una ecuación en diferencias para s_k es
$$\binom{n}{0}s_k = \binom{n}{1}s_{k-1} - \binom{n}{2}s_{k-2} + \binom{n}{3}s_{k-3} - \cdots + (-1)^n\binom{n}{n-1}s_{k-(n-1)} + (-1)^{n+1}\binom{n}{n}s_{k-n},$$

[73] *Vid*. pág. 1130 de esta edición.
[74] *Vid. v. gr.* https://es.wikipedia.org/wiki/Principio_de_inclusi%C3%B3n-exclusi%C3%B3n#Caso_especial.

la cual, en forma estándar, es

$$s_k - n s_{k-1} + \binom{n}{2} s_{k-2} - \binom{n}{3} s_{k-3} + \cdots + (-1)^{n-2}\binom{n}{n-2} s_{k-(n-2)} + (-1)^{n-1} n s_{k-(n-1)} + (-1)^n s_{k-n} = 0,$$

que una expresión explícita para su solución general es

$$s_k = c_n k^{n-1} + c_{n-1}k^{n-2} + \cdots + c_3 k^2 + c_2 k + c_1,$$

con $c_1, c_2, \ldots, c_n \in \mathbb{R}$, y que una expresión explícita de la solución particular de la situación en estudio es

$$s_k = \binom{k+n-1}{n-1}. \qquad \blacksquare$$

Observación 20.8.0.— Pudiésemos utilizar Wolfram|Alpha[75] para confirmar la solución general de (20.122). Introduciendo `s(k)=((k+n-1)/k)*s(k-1)`, este artefacto en línea nos informa que la expresión explícita de dicha solución general es

$$s_k = c \cdot \frac{(n+1)^{\overline{k-1}}}{k!} \quad (c \in \mathbb{R}),$$

donde el numerador es el factorial ascendente, expresión que simplificamos demostrando que es justo la anterior:

$$\begin{aligned}
s_k &= c \cdot \frac{(n+1)^{\overline{k-1}}}{k!} \\
&= c \cdot \frac{(n+1)\cdot(n+2)\cdot \ldots \cdot((n+1)+(k-2)-1)\cdot((n+1)+(k-1)-1)}{k!} \\
&= c \cdot \frac{1}{k!}\cdot(n+1)\cdot(n+2)\cdot \ldots \cdot(n+k-2)\cdot(n+k-1) \\
&= c \cdot \frac{1}{k!}\cdot(k+n-1)\cdot(k+n-2)\cdot(n+2)\cdot(n+1) \\
&= c \cdot \frac{1}{k!}\cdot\frac{(k+n-1)!}{n!} \\
&= c \cdot \frac{(k+n-1)!}{k!\cdot n\cdot(n-1)!} \\
&= c \cdot \frac{1}{n}\cdot\frac{(k+n-1)!}{k!\cdot(n-1)!} \quad (c \in \mathbb{R}).
\end{aligned}$$

Observación 20.8.1.— Pudiésemos comprobar la solución del PVI, por ejemplo, introduciendo el problema de valores iniciales `s(k)=((k+n-1)/k)*s(k-1), s(1)=n` en el artefacto en línea Wolfram|Alpha.

Observación 20.8.2.— Utilizamos el artefacto en línea SageMath[76] y este programita en lenguaje Sage para calcular la solución general de una ecuación en diferencias lineal con coeficientes constantes.

---

[75] *Vid*. https://www.wolframalpha.com/.
[76] *Cfr. supra* § 11 (pág. cii de esta edición).

```
# Ejecutar en: Sage Cell Server: https://sagecell.sagemath.org/
#
def solgeneral(ecdif):
n = len(ecdif)-1
policar = ecdif[0]*x^n + sum([ecdif[i+1]*x^(n-1-i) for i in range(n)])
raicar = policar.roots()
vars = [var('c'+str(i+1)) for i in range(n)]
var('k')
dev = 0
for r in raicar:
# r = (r[0],r[1]), en la forma (raíz, multiplicidad)
polisol = sum([vars.pop(0)*k^i for i in range(r[1])])
dev += polisol*r[0]^k
return dev
```

Observación 20.8.3.— El programita de la observación 20.8.2 (pág. 1419 de esta edición) y a continuación

```
{show(solgeneral([1,-2,1]))
```

muestra $c_2k + c_1$ como una expresión explícita de la solución general de (20.124).

Observación 20.8.4.— El programita de la observación 20.8.2 (pág. 1419 de esta edición) y a continuación

```
show(solgeneral([1,-3,3,-1]))
```

muestra $c_3k^2 + c_2k + c_1$ como una expresión explícita de la solución general de (20.126).

Ejemplo 762

Sean $k, n \in \mathbb{Z}^+$. Dada la disposición ordenada original $D_k = (o_1, o_2, \ldots, o_k)$ de k objetos distinguibles, diremos que una permutación σ (*sigma*) de dichos objetos es una *permutación cercana* de D_k de grado n, si todo objeto en σ está a menos de n posiciones de su posición original en D_k y diremos que una permutación σ de dichos objetos es una *permutación lejana* de D_k de grado n si todo objeto en σ está a más de n posiciones de su posición original en D_k. Dicho esto, nos proponemos lo siguiente: si c_k representa el número de permutaciones cercanas de D_k de grado 2, hallar una ecuación en diferencias para c_k y enontrar finalmente una expresión explícita tan simple como sea posible para c_k.

[EFE 14.7.2020:4a (p.h.e.c.)].

Resolución.— Si o_k está en la última posición, el problema se reduce a las permutaciones cercanas de $D_{k-1} = (o_1, o_2, \dots, o_{k-1})$ de grado 2, por lo que hay c_{k-1} formas de permutar los objetos con o_k fijo en la última posición. Por otro lado, si o_{k-1} está en la última posición, obligatoriamente o_k debe estar en la penúltima (ya que debe estar a menos de dos posiciones de su posición original en D_k), por lo que el problema se reduce a las permutaciones cercanas de $D_{k-2} = (o_1, o_2, \dots, o_{k-2})$ de grado 2, por lo que hay c_{k-2} formas de permutar los objetos con o_{k-1} fijo en la última posición. Por tanto, por el principio de la adición [¡esto requiere justificación! ✍],

$$c_k = c_{k-1} + c_{k-2},$$

para k entero, $k \geq 3$.

Por otro lado, $c_1 = 1$ —sólo la disposición original (o_1)— y $c_2 = 2$ —las disposiciones (o_1, o_2) y (o_2, o_1)—.

Para este problema de valores iniciales, la solución explícita es

$$c_k = F_{k+1},$$

siendo F_n los números de Fibonacci[77], esto es[78],

$$c_k = \frac{\phi^{k+1} - (1-\phi)^{k+1}}{\sqrt{5}},$$

siendo $\phi = (1+\sqrt{5})/2$ el número áureo. ■

Actividad 20.29

En el ejemplo inmediatamente anterior hemos aplicado el principio de la adición, mas esto requiere una justificación de cómo hemos procedido; elaborarla es una actividad necesaria, además de conveniente; hagámoslo.

§ 20.9 Bibliografía

Las obras que he considerado adecuadas para una aproximación inicial, para saber más, para una profundización acullá y para la práctica de la combinatoria, lo son también para las ecuaciones en diferencias.

- En español:

[32] Félix García Merayo. *Matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 2015.

[77] *Cfr.* https://oeis.org/A000045.
[78] *Cfr.* https://es.wikipedia.org/wiki/Sucesi%C3%B3n_de_Fibonacci#F%C3%B3rmula_expl%C3%ADcita.

[124] Jiří MATOUŠEK y Jaroslav NEŠETŘIL. *Invitación a la matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2008.

[151] Kenneth Howard ROSEN. *Matemática discreta y sus aplicaciones*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 5.ª ed., 2004. (La 5.ª edición es la última en español).

[155] Ralph Peter GRIMALDI. *Matemáticas discreta y combinatoria*. Addison-Wesley Iberoamericana, Wilmington, New Castle, Delaware (US-DE), Estados Unidos de América, 3.ª ed., 1997.

[156] Juan Carlos FERRANDO PÉREZ y Valentín GREGORI GREGORI. *Matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2.ª ed., 2012.

[157] Kenneth Allen ROSS y Charles Richard Bowers WRIGHT. *Matemáticas discretas*. Prentice-Hall Hispanoamericana, Naucalpan de Juárez, Estado Libre y Soberano de México (MX-MEX), Estados Unidos Mexicanos, 2.ª ed., 1990.

[214] José Ramón FRANCO BRAÑAS, María Candelaria ESPINEL FEBLES y Pedro Ramón ALMEIDA BENÍTEZ. *Manual de combinatoria*. Dirección General de Universidades e Investigación del Gobierno de Canarias, La Laguna - Tenerife, Canarias (ES-CN), España, 2005.

- En inglés:

[152] Kenneth Howard ROSEN. *Discrete Mathematics and its Applications*. McGraw-Hill, Nueva York, Nueva York (US-NY), Estados Unidos de América, 7.ª ed., 2012.

[158] Richard JOHNSONBAUGH. *Discrete Mathematics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 8.ª ed., 2018.

[190] James BRADLEY. *Introduction to discrete mathematics*. Addison-Wesley, Reading, Middlesex, Mancomunidad de Massachusetts (US-MA), Estados Unidos de América, 1988.

[217] Richard Anthony BRUALDI. *Introductory Combinatorics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 5.ª ed., 2010.

[218] Peter Jephson CAMERON. *Notes on combinatorics*. Autopublicación, 2013.

[219] Kenneth Paul BOGART. *Combinatorics throuhg guided discovery*. Autopublicación, 2004.

- Junto a las siguientes, que están dedicadas esencialmente a la práctica:

[150] Félix GARCÍA MERAYO, Gregorio HERNÁNDEZ PEÑALVER y Antonio NEVOT LUNA. *Problemas resueltos de matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 2018.

[154] Carlos GARCÍA GÓMEZ, Josep María LÓPEZ BESORA y Dolors PUIGJANER RIBA. *Matemática discreta*. Pearson Educación, Madrid, Comunidad de Madrid (ES-M), España, 2002.

[213] Felicidad Aguado Martín, Felipe Gago Couso, Manuel Ladra González, Gilberto Pérez Vega, Concepción Vidal Martín y Ana María Vieites Rodríguez. *Problemas resueltos de Combinatoria. Laboratorio con SageMath*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2018.

Apéndices

La frase proverbial «el saber no ocupa lugar y, por mucho que tengas, lo puedes aumentar» y el refrán «más vale la práctica que la gramática» hacen causa común para el afloramiento de estos aditamentos.



Algo *in itinere*, algo *ex post*

Perdóname, no sé decirte nada más, pero tú comprende que yo aún estoy en el camino.
(José Agustín GOYTISOLO, *Palabras para Julia*).

Lo cierto es que si bien las actividades de § A.0 pudiesen situarse en el camino y, por lo tanto, son abordables desde el estudio de estas notas, las de § A.2–§ A.4 residen, mucho más que menos, en su exterior, más allá de los márgenes de estas notas, si bien esto no impide que gocemos del conocimiento que acompaña a su exploración. Que siendo cierto el tópico «la experiencia es la madre de la ciencia», nada es comparable con aprender mientras investigamos.

§ A.0 Propuesta de actividades finales *in itinere*

Actividad A.0

Pruebas de asociatividad.— (`Proyecto de programación`). Interesémonos por las implementaciones de la *prueba de asociatividad de* LIGHT[*] y de la *prueba de asociatividad de* ABDALI para operaciones conmutativas[†], y ofrezcamos las nuestras (el lenguaje de programación es a nuestra entera elección; eso sí, no olvidemos documentar el código).

[*] *Vid. v. gr.* https://en.wikipedia.org/wiki/Light%27s_associativity_test.

[†] *Vid*. https://www.jstor.org/stable/3613856 (este artículo es accesible, por ejemplo, desde el dominio de la Universidad de Extremadura, `unex.es`).

Actividad A.1

Juntores como matrices.— Representemos:

- un valor de verdad como una matriz 2×1, Falso (F) $= \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ y Verdadero (V) $= \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, que pudiésemos abreviar por $|0\rangle$ y $1\rangle$ (ket cero y ket uno, en notación de Dirac)[*];
- los posibles valores de verdad de una variable proposicional como la matriz 2×2, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, esto es, la yuxtaposición de las matrices 2×1, F y V anteriores;
- los posibles valores de verdad de dos variables, p y q, como la matriz 2×4, $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, esto es, la yuxtaposición de las matrices 2×2 correspondientes a los p y q anteriores.

Con esta representación, es posible hallar los valores de verdad de, digamos, $p \wedge q$, encontrando una matriz 4×4 adecuada por la que multiplicar la matriz 2×4 anterior; en efecto, la matriz resultante del producto

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

no es más que F F F V, en definitiva, $p \wedge q$.

Nos preguntamos:

0. ¿Cuántas matrices binarias 4×4 hay? En general, ¿cuántas matrices binarias $n \times n$ hay?
1. ¿Cuántas matrices binarias 4×4 tienen determinante uno? En general, ¿cuántas matrices binarias $n \times n$ tienen determinante uno?
2. `Proyecto de programación.—` (El lenguaje de programación es a nuestra entera elección; debemos documentar el código).
   I. ¿Cómo interpretamos la última matriz 2×4, esto es, a qué par de valores de verdad de p y q corresponde cada columna (las cuatro columnas son F, F, F y V?
   II. ¿Puede la matriz 2×4 correspondiente a $p \wedge q$ ser generada por otra matriz 4×4?
   III. Sobre esto último, ¿qué sucede con los demás juntores diádicos?
   IV. En definitiva, para cada matriz 2×4 correspondiente a un juntor diádico se trata de encontrar, caso de que sea posible, todas las matrices binarias 4×4 (llamémoslas sus asociadas) que la generan.
   V. ¿Ha sido posible hacerlo para todos los juntores? ¿Por qué?
   VI. Entonces, ¿detectamos algún patrón entre las matrices 2×4 y sus asociadas?

[*] *Cfr. supra* § 9.3 (pág. 522 de esta edición).

Actividad A.2

Matemática discreta en la naturaleza.— Análisis matemático y crítico de *Nature by Numbers* —cortometraje inspirado en los números, la geometría y la naturaleza— (Cristóbal Vila, 2010) (https://etereaestudios.com/works/nature-by-numbers/). Puntos de partida:

- el propio vídeo;
- la información proporcionada en dicha página web sobre la matemática subyacente a lo que aparece en dicho cortometraje —más trabajos de Cristóbal Vila, en su galería de trabajos de Etérea (https://etereaestudios.com/works/)—.

Actividad A.3

Mentiras, malditas mentiras y estadísticas: lo dicen los números, no lo digo yo.— (Impromptu estadístico). Análisis matemático y crítico sobre la generación de mentiras a partir de la lectura, interpretación o manipulación errónea, malintencionada o no, del diseño de un experimento, del análisis de los datos, del análisis de los resultados, de la presentación de los datos y resultados, etc. Puntos de partida:

- Conferencias:
  - Sebastian Wernicke: *Lies, damned lies and statistics (about TEDTalks)* («Mentiras, sucias mentiras y estadísticas [sobre las charlas TED]») (https://www.ted.com/talks/sebastian_wernicke_lies_damned_lies_and_statistics_about_tedtalks) (© CC BY-NC-ND 4.0 Internacional);
  - Peter Donnelly: *How juries are fooled by statistics* («Cómo engañan a los jurados con las estadísticas») (https://www.ted.com/talks/peter_donnelly_how_juries_are_fooled_by_statistics) (© CC BY-NC-ND 4.0 Internacional);
  - Lista de reproducción de TED: *Making sense of too much data* («Dando sentido a demasiados datos») (https://www.ted.com/playlists/56/making_sense_of_too_much_data) (© CC BY-NC-ND 4.0 Internacional).
- Libros:
  - Darrell Huff y Irving Geis (1954): *How to Lie with Statistics* («Cómo mentir con estadísticas»; traducción de Octavio Freixas Ortega) (© TDR).
- Películas:
  - *Magic Town* («Ciudad mágica») (1947, RKO Pictures); dirigida por William Augustus Wellman; guión de Robert Riskin, basada en una historia escrita por Robert Riskin y Joseph Krumgold; producida por Robert Riskin; reparto: James Stewart, Jane Wyman, Kent Smith, Ned Sparks, Wallace Ford y otros (http://en.wikipedia.org/wiki/Magic_Town) (© TDR).

Actividad A.4

Laberintos tridimensionales.— `(Proyecto de programación)`. A la búsqueda de algo-

ritmos de generación, representación y resolución de laberintos tridimensionales. Puntos de partida:

- algoritmos de generación: https://en.wikipedia.org/wiki/Maze_generation_algorithm;
- algoritmos de resolución: https://en.wikipedia.org/wiki/Maze-solving_algorithm;
- esta publicación: https://blog.koehntopp.info/2021/01/10/labyrinths-in-python.html;
- esta conversación en Reddit: https://www.reddit.com/r/VoxelGameDev/comments/1lubqpe/looking_for_a_3d_maze_generation_algorithm/.

Actividad A.5

Inversión de código.— `(Proyecto de computación).` «¿No sería fantástico poder ejecutar un programa al revés o, mejor aún, derivar de un programa P un segundo programa P^{-1} que calcule el inverso de P? Esto significaría que ejecutar P seguido de P^{-1} sería lo mismo que no ejecutar ningún programa. Además, si tuviésemos el resultado de ejecutar P, pero perdiésemos la entrada, podríamos ejecutar P^{-1} para determinar esa entrada.» Así comienza el capítulo 21 de *The Science of Programming* de David Gries. Puntos de partida:

- capítulo 21 de *The Science of Programming* de David Gries: https://link.springer.com/chapter/10.1007/978-1-4612-5983-1_22;
- computación reversible: https://en.wikipedia.org/wiki/Reversible_computing;
- autómata celular reversible: https://en.wikipedia.org/wiki/Reversible_cellular_automaton;
- los modelos de lenguaje son invertibles (13.3.2026): Giorgos Nikolaou, Tommaso Mencattini, Donato Crisostomi, Andrea Santilli, Yannis Panagakis y Emanuele Rodolà, *Language Models are Injective and Hence Invertible*: https://arxiv.org/abs/2510.15511;
- Proyecto Fin de Carrera de Ingeniería Informática *Inversión de código* de Juan Manuel Martín Alonso, Escuela Politécnica, Universidad de Extremadura, Cáceres, diciembre de 2000.

Actividad A.6

Azar.— `(Proyecto de computación).` Simular el azar, ¿quién no quisiese? Puntos de partida:

- generación de números aleatorios: https://en.wikipedia.org/wiki/Random_number_generation;
- ANU QRNG *Quantum random numbers*: https://qrng.anu.edu.au/;
- Trabajo Fin de Carrera de Diplomatura en Informática *Generación de números aleatorios* de María Inés Pulido Maestre, Escuela Universitaria Politécnica, Universidad de Extremadura, Cáceres, septiembre de 1993.

Actividad A.7

Dilema del prisionero iterado.— `(Proyecto de computación)`. El estudio de la iteración del dilema del prisionero parece ser esencial para la comprensión de la cooperación, la confianza y la traición en las relaciones humanas. Puntos de partida:

- https://en.wikipedia.org/wiki/Prisoner%27s_dilemma;
- Proyecto Fin de Carrera de Diplomatura en Informática *El dilema del preso iterado* de Trinidad SERRADILLA RODRÍGUEZ, Escuela Universitaria Politécnica, Universidad de Extremadura, Cáceres, septiembre de 1994.

Actividad A.8

Matemáticas automatizadas.— Inicio de la lectura y redacción optativa de un breve análisis matemático y computacional, reflexivo, crítico y analítico, sobre:

- Alexander Keewatin DEWDNEY (1993), *The Tinkertoy Computer and other machinations*, capítulo 17 (*Automated Math*), Nueva York: W. H. Freeman. (En inglés) (https://archive.org/details/tinkertoycomputer00dewd). (Juegos de ordenador. De cómo un par de programas obtusos pasan por genios en los tests de inteligencia. *Investigación y Ciencia*, n.º 116, mayo 1986, págs. 94–98, Prensa Científica, S. A. [En español]).

Actividad A.9

Conjetura de Collatz.— Inicio de la búsqueda de información y redacción optativa de un breve análisis matemático y computacional, reflexivo, crítico y analítico, sobre la conjetura de Collatz y sobre su «visualización». Puntos de partida:

- *Vid. supra* cuadro azul Conjetura de Collatz (pág. 1095 de esta edición);
- Jason DAVIES (2012), *Collatz Graph: All Numbers Lead to One* (https://www.jasondavies.com/collatz-graph/);
- Kazuhito OWADA (2025), *Collatz Trees: A Structural Framework for Understanding the 3x+1 Problem* (https://www.preprints.org/manuscript/202504.1491/v1).

Actividad A.10

Proyecto y plan de aprendizaje.— Durante los años académicos 2016–2017 al 2022–2023 estuvo supervisado el proyecto de aprendizaje Matemática Discreta y Numérica (https://es.wikipedia.org/wiki/Wikipedia:Proyecto_educativo/Matemática_discreta_y_numérica), con su plan de aprendizaje asociado (https://es.wikipedia.org/wiki/Wikipedia:Proyecto_educativo/Matemática_discreta_y_numérica/Plan_de_aprendizaje), el cual cumplía con todos los requerimientos esenciales del plan docente de la asignatura Ampliación de Matemáticas impartida en la Escuela Politécnica de la Universidad de Extremadura. Wikipedia es un sitio wiki público, libre y abierto, por lo que fuera de dicho rango académico de fechas, debido a tal naturaleza, *el proyecto permanece siempre abierto públicamente —sintámonos libres de contribuir a*

él—; en otras palabras, la componente de aprendizaje de este proyecto nunca termina pues *la cooperación voluntaria carece de plazo*.

§ A.1 Bibliografía *in itinere*/*ex post*

Para saciar algunas de nuestras inquietudes remanentes o no conscientes (aún).

- Sobre números «famosos»« o interesantes»:
  - Tres libros:
    - *El Numeronomicón*, de Josep María ALBAIGÈS (https://www.tebarflores.com/matematicas/239-el-numeronomicon-diccionario-de-numeros-sus-propiedades-matematicas-tradicion-historica-y-simbolismo-9788473605540.html);
    - *Les nombres remarquables*, de François LE LIONNAIS (https://www.editions-hermann.fr/livre/9782705614072) (figura como bibliografía, no referenciada, en https://fr.wikipedia.org/wiki/Nombre_remarquable#Bibliographie);
    - *The Penguin dictionary of curious and interesting numbers*, de David WELLS (https://en.wikipedia.org/wiki/The_Penguin_Dictionary_of_Curious_and_Interesting_Numbers);
  - en Mathigon es posible ver el almanaque de los números interesantes (https://mathigon.org/almanac), donde introduciendo un número abajo y pulsando la tecla de Retorno de carro / Enter / Intro [⟵], nos situaremos en dicho número y veremos además algunos de los más cercanos;
  - algunos que se destacan en Wikipedia:
    - https://en.wikipedia.org/wiki/List_of_numbers#Mathematical_significance;
    - https://en.wikipedia.org/wiki/List_of_numbers#Cultural_or_practical_significance;

    algunos con nombre propio (https://en.wikipedia.org/wiki/List_of_numbers#Named_numbers), si bien pudiésemos considerar interesantes a todos los números (https://en.wikipedia.org/wiki/Interesting_number_paradox).
- Sobre teoría de números, combinatoria y más, pudiésemos echar un ojo a estas páginas (u otras similares):
  - *Olimpiadas de matemáticas. Página de preparación y problemas*, de José Miguel MANZANO: https://wpd.ugr.es/~jmmanzano/preparacion/problemas.php?page=1&d=-1&c=1 (contiene una amplia variedad de ejercicios resueltos sobre teoría de números, combinatoria, juegos y estrategias, etc., pudiendo elegir hasta cinco grados de dificultad; además, tiene apuntes);

  - *Olimpiada matemática española. Problemas propuestos y resultados*, de Carles ROMERO: http://www.olimpiadamatematica.es/platea.pntic.mec.es/_csanchez/olimprab.htm;
  - *Princeton University Mathematics Competition* (PUMaC) *Problem and Result Archive*: https://jason-shi-f9dm.squarespace.com/archives;
  - *International Mathematics Competition for University Students*: https://www.imc-math.org.uk/.

- Y suplementándolos:
  - MathNet (*A Global Multimodal Benchmark for Mathematical Reasoning and Retrieval*) (https://mathnet.csail.mit.edu/), un compendio de cerca de 31 000 problemas con sus soluciones, procedentes de Olimpiadas Matemáticas, de 47 países, en 17 idiomas y 20 años de competición.

§ A.2 Propuesta de actividades finales *ex post*

Las siguientes actividades son para quienes tengamos inquietudes investigadoras; démonos la bienvenida a un periplo que de seguro disfrutaremos, rastreando, rebuscando, y reflexionando.

Miscelánea de entrantes.

Actividad A.11

Números regulares (números de HAMMING).— Punto de partida:

- https://en.wikipedia.org/wiki/Regular_number.

Actividad A.12

Cuadrados mágicos.— Punto de partida:

- https://en.wikipedia.org/wiki/Magic_square.

Actividad A.13

Cuadrados latinos.— Punto de partida:

- https://en.wikipedia.org/wiki/Latin_square.

Actividad A.14

División de enteros largos.— Puntos de partida:

- https://en.wikipedia.org/wiki/Division_algorithm#Long_division;
- https://en.wikipedia.org/wiki/Division_algorithm#Fast_division_methods;

- https://en.wikipedia.org/wiki/Fourier_division.

Actividad A.15

Juegos matemáticos y no matemáticos.— Los matemáticos: deben terminar en un número finito de jugadas; no influye el azar; quien juegue puede observar todos los movimientos: juegos: Hit & Run (Jurg NIEVERGELT); Connecto (David L. SILVERMAN, *Your move*, McGraw-Hill, 1971); Bridg-It (David GALE, https://en.wikipedia.org/wiki/Shannon_switching_game); juego de los bloques deslizantes. Los no matemáticos propuestos son las damas y el dominó. Puntos de partida:

- *Circo Matemático*, de Martin GARDNER, Alianza editorial, 1983;
- Alexander Keewatin DEWDNEY, Computer Recreations, *Scientific American*, Julio de 1984: A program that plays checkers can often stay one jump ahead, https://www.scientificamerican.com/article/computer-recreations-1984-07/;
- Trabajo Fin de Carrera de Diplomatura en Informática *Juegos matemáticos: Hit & Run, Connecto y Bridg-It* de Margarita COLLADO SIERRA, Escuela Politécnica, Universidad de Extremadura, Cáceres, septiembre de 1998;
- Trabajo Fin de Carrera de Diplomatura en Informática *Hip-Bloq* de José Antonio GARCÍA LÓPEZ, Escuela Universitaria Politécnica, Universidad de Extremadura, Cáceres, septiembre de 1995;
- Trabajo Fin de Carrera de Diplomatura en Informática *Una solución al juego de damas* de Higinio HERNÁNDEZ BARBERO, Escuela Politécnica, Universidad de Extremadura, Cáceres, septiembre de 1990;
- Trabajo Fin de Carrera de Diplomatura en Informática *Dominó: solitarios y juego de parejas* de Juan Pedro ESCANDÓN DE GAMA, Escuela Politécnica, Universidad de Extremadura, Cáceres, febrero de 1996;
- Trabajo Fin de Carrera de Diplomatura en Informática *Dominó: juego de parejas y solitarios* de José Antonio ESCANDÓN DE GAMA, Escuela Politécnica, Universidad de Extremadura, Cáceres, febrero de 1996.

Actividad A.16

División de enteros largos.— Puntos de partida:

- https://en.wikipedia.org/wiki/Division_algorithm#Long_division;
- https://en.wikipedia.org/wiki/Division_algorithm#Fast_division_methods;
- https://en.wikipedia.org/wiki/Fourier_division.

Actividad A.17

Multiplicación de matrices.— El algoritmo de STRASSEN y el resto de algoritmos de multi-

plicación rápida de matrices requieren para su funcionamiento de la estructura de anillo. Puntos de partida:

- https://en.wikipedia.org/wiki/Strassen_algorithm;
- https://en.wikipedia.org/wiki/Matrix_multiplication_algorithm.

Actividad A.18

Dibujo de árboles.— Punto de partida:

- https://www.cs.unc.edu/techreports/89-034.pdf.

Actividad A.19

Cálculos de calendarios.— Punto de partida:

- https://reingold.co/calendars.shtml.

Probabilidad.

Actividad A.20

Cadenas de Markov y modelos ocultos de Markov.— Puntos de partida:

- https://en.wikipedia.org/wiki/Markov_chain;
- https://en.wikipedia.org/wiki/Hidden_Markov_model.

Análisis de decisión.

Actividad A.21

Árboles de decisión y diagramas de influencia.— Puntos de partida:

- https://en.wikipedia.org/wiki/Decision_tree;
- https://en.wikipedia.org/wiki/Influence_diagram.

Optimización matemática.

Actividad A.22

Problema de la dieta.— Punto de partida:

- https://en.wikipedia.org/wiki/Stigler_diet.

Actividad A.23

Programación entera.— Puntos de partida:

- https://en.wikipedia.org/wiki/Integer_programming;
- Trabajo Fin de Carrera de Diplomatura en Informática *La programación entera* de Rufina Ortega Alegre, Escuela Universitaria Politécnica, Universidad de Extremadura, Cáceres, septiembre de 1991.

Actividad A.24

Construcción de horarios.— Puntos de partida:

- https://en.wikipedia.org/wiki/Schedule;
- https://pure.tue.nl/ws/files/1849715/200211248.pdf;
- https://isd.ktu.lt/it2010/material/Proceedings/3_FM_5.pdf;
- Trabajo Fin de Carrera de Diplomatura en Informática *Algoritmos de vuelta atrás* de Antonio Salazar Carmona, Escuela Universitaria Politécnica, Universidad de Extremadura, Cáceres, febrero de 1995.

Actividad A.25

Problema de la mochila.— Punto de partida:

- https://en.wikipedia.org/wiki/Knapsack_problem;
- Jesús Ángel Velázquez Iturbide, Un problema combinatorio y su resolución con cinco técnicas algorítmicas, *Novática* 118, págs. 103–109, 1995 (http://www2.ati.es/novatica/1995/nov-dic/Nv118-Digital.pdf).

Actividad A.26

Problema del corte de valores (*cutting-stock*).— Punto de partida:

- https://en.wikipedia.org/wiki/Cutting_stock_problem.

Ingeniería del software.

Actividad A.27

Programación literaria y programación aclarativa/elucidativa/explicativa.— Puntos de partida:

- https://en.wikipedia.org/wiki/Literate_programming;
- http://www.literateprogramming.com/;
- https://homes.cs.aau.dk/~normark/elucidative-programming/.

Actividad A.28

Especificaciones ejecutables.— Puntos de partida:

- Fuchs, Norbert E., *Specifications Are (Preferably) Executable*, https://lim.univ-reunion.fr/staff/fred/Enseignement/Verif-M2/Articles/Executable_Specifications-Fuchs-1992.pdf;
- https://genexus.blog/es_ES/genexus-platform/executable-specifications-and-four-decades-of-genexus-vision/;
- https://es.linkedin.com/pulse/la-democratizaci%C3%B3n-del-software-programar-es-beatriz-mart%C3%ADn-valc%C3%A1rcel-aq4ef.

Actividad A.29

Lenguajes de expresión de derechos.— Puntos de partida:

- https://en.wikipedia.org/wiki/Creative_Commons_Rights_Expression_Language;
- Proyecto Fin de Carrera de Ingeniería Informática *Filtros de contenidos basados en REL* de Ángel Vivas Vivas, Escuela Politécnica, Universidad de Extremadura, Cáceres, septiembre de 2010.

Actividad A.30

Conversión de datos.— Puntos de partida:

- https://en.wikipedia.org/wiki/Data_conversion;
- Proyecto Fin de Carrera de Ingeniería Informática *Transformación de formatos de archivos* de José Antonio Cordero García, Escuela Politécnica, Universidad de Extremadura, Cáceres, septiembre de 2010.

Ciencia computacional teórica.[°]

Actividad A.31

Verificación formal.— Punto de partida:

- https://en.wikipedia.org/wiki/Formal_verification.

Actividad A.32

Teoría de la computabilidad.— Puntos de partida:

- https://en.wikipedia.org/wiki/Computability_theory;
- https://plato.stanford.edu/entries/turing-machine/;
- https://plato.stanford.edu/entries/computability/.

Actividad A.33

Teoría de la complejidad computacional.— Puntos de partida:

- https://en.wikipedia.org/wiki/Computational_complexity_theory;
- https://en.wikipedia.org/wiki/NP-completeness; https://en.wikipedia.org/wiki/Complexity_class;
- https://plato.stanford.edu/entries/computability/.

Actividad A.34

El problema del viajante y el problema de enrutamiento de vehículos.— Puntos de partida:

- https://en.wikipedia.org/wiki/Travelling_salesman_problem;

[°] *Cfr. v. gr.* https://en.wikipedia.org/wiki/Theoretical_computer_science.

- https://en.wikipedia.org/wiki/Vehicle_routing_problem;
- https://en.wikipedia.org/wiki/Traffic_flow;
- https://en.wikipedia.org/wiki/Traffic_optimization;
- Trabajo Fin de Carrera de Diplomatura en Informática *Optimización de rutas (Rutero)* de María Isabel Barriga Franco, Escuela Universitaria Politécnica, Universidad de Extremadura, Cáceres, septiembre de 1989;
- Trabajo Fin de Carrera de Diplomatura en Informática *Estudio sobre el tráfico en Cáceres* de Antonio Puerto Godino, Escuela Universitaria Politécnica, Universidad de Extremadura, Cáceres, junio de 1991.

Actividad A.35

Castor afanoso.— Puntos de partida:

- https://en.wikipedia.org/wiki/Busy_beaver;
- https://www.quantamagazine.org/busy-beaver-hunters-reach-numbers-that-overwhelm-ordinary-math-20250822/;
- https://bbchallenge.org/~pascal.michel/bbc;
- https://opensource.com/article/21/5/busy-beaver-game-c.

Actividad A.36

Constante de Chaitin.— Puntos de partida:

- https://en.wikipedia.org/wiki/Algorithmic_information_theory;
- https://en.wikipedia.org/wiki/Chaitin%27s_constant.

Razonamiento combinatorio.

Actividad A.37

Discusión del ejemplo 761 (pág. 1412 de esta edición).— Discutamos lo propuesto en él para el caso general de coeficientes naturales, esto es, para $a_1x_1 + a_2x_2 + \cdots + a_nx_n = k$, con $a_1, a_2, \ldots, a_n \in \mathbb{N}$.

[EFO 12.6.2020:4b (p.h.e.c.)].

Actividad A.38

Discusión del ejemplo 762 (pág. 1420 de esta edición).— Con respecto a él y si l_k representa el número de permutaciones lejanas de D_k de grado 2, discutamos el hallar una ecuación en diferencias para l_k y encontrar finalmente una expresión explícita tan simple como sea posible para l_k.

[EFE 14.7.2020:4b (p.h.e.c.)].

Actividad A.39

Problema de las esposas y las llaves (*Key party problem*).— Punto de partida:

- El problema de las esposas y las llaves, de Josefina Álvarez y Lorenz Hughes, publicado en *Miscelánea Matemática* 61, 31–42, 2015; disponible en: https://miscelaneamatematica.org/download/tbl_articulos.pdf2.a7676da54b3699e7.363130342e706466.pdf.

Miscelánea de ingredientes.

Actividad A.40

El algoritmo PageRank de Google.— Un caso de optimización de búsquedas de páginas web cuyos ingredientes son la teoría de grafos, la probabilidad y el álgebra lineal. Punto de partida:

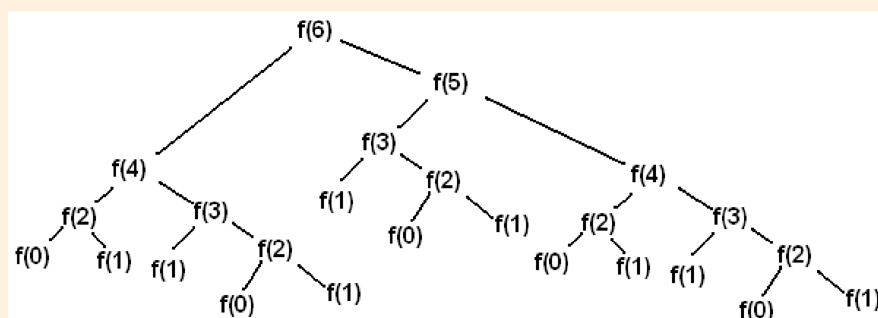
- Pablo Fernández Gallardo, El secreto de Google y el álgebra lineal, en el curso *Sociedad, Ciencia, Tecnología y Matemáticas 2006*, https://sctmates.webs.ull.es/modulo1lp/8/pfernandez.pdf.

Además de todas estas actividades que han precedido en este subcapítulo, contamos con las correspondientes a las **imágenes de portadas anteriores** de estas notas, a lo largo de sus sucesivas ediciones, que, hasta el momento presente, han sido las que aparecen en las tres siguientes actividades. Cada una de estas imágenes recoge una situación de interés que seguramente despertará nuestra inquietud por saber más de ella. Que nos informemos y aprendamos de su temática, completa el conjunto de actividades *ex post* propuestas.

Actividad A.41

Memoización y programación dinámica.— Puntos de partida:

- https://en.wikibooks.org/wiki/Algorithms/Dynamic_Programming;
- https://en.wikipedia.org/wiki/Memoization;
- https://en.wikipedia.org/wiki/Dynamic_programming.

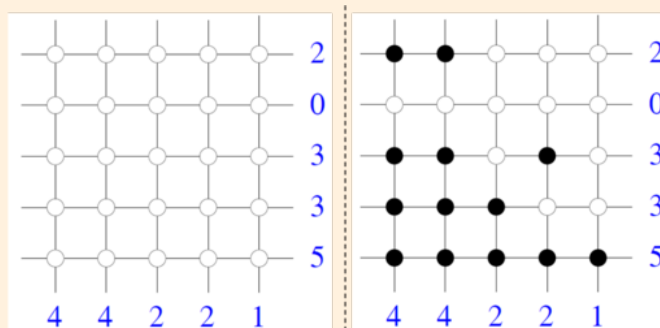


Un ejemplo de árbol-traza para el sexto número de Fibonacci (imagen de NatasaVuksanovic123, https://commons.wikimedia.org/wiki/File:Algorithms-F6Call-Tree.png).

Actividad A.42

Tomografía discreta.— Punto de partida:

- https://en.wikipedia.org/wiki/Discrete_tomography.

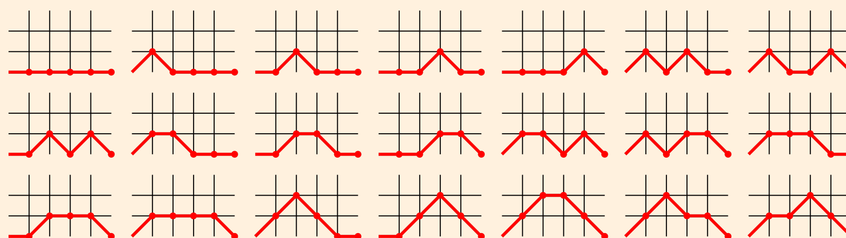


(Imagen de AAlpers, https://commons.wikimedia.org/wiki/File:Discrete_tomography.png).

Actividad A.43

Números de Motzkin.— Punto de partida:

- https://es.wikipedia.org/wiki/Número_de_Motzkin.



Una interpretación de los números de Motzkin (imagen de de Mrmw, https://commons.wikimedia.org/wiki/File:Motzkin5.svg).

§ A.3 Bibliografía *ex post*

Ex post (para su lectura e investigación posterior por parte del alumnado).

En inglés.

[222]Mykel J. KOCHENDERFER, Tim A. WHEELER y Kyle H. WRAY. *Algorithms for Decision Making*. The MIT Press, Cambridge, Massachusetts, Estados Unidos, 2022. http://algorithmsbook.com/files/dm.pdf (accedido el 19.1.2026). ©CC BY-NC-ND.

[223]Pascal MICHEL. The Busy Beaver Competition: a historical survey. *arXiv*, página 0906.3749, 2022.

[224]*The Electronic Journal of Combinatorics*, 2024. http://www.combinatorics.org/ojs/index.php/eljc/index (accedido el 26.1.2024). ©gratis OA.

[225]Terry TAO. *What's new*, 2024. blog de Terence Tao, Mozart of maths. https://terrytao.wordpress.com/ (accedido el 26.1.2024). ©gratis OA.

§ A.4 Mucho más allá: los siete problemas del milenio

Pues sí, mucho más allá, pero por si tuviésemos inquietud en los siete problemas del milenio o en alguno en particular (quizás el más cercano a la matemática discreta sea el que aborda la relación entre las clases de complejidad P y NP), creo que, además de toda la información (en inglés) que hay sobre cada uno de ellos en el sitio web del *Clay Mathematics Institute*[1] (la institución que ofrece un premio de un millón de dólares por cada uno que se resuelva —por ahora, sólo se da por resuelta la conjetura de POINCARÉ, demostrada por Grigori PERELMAN[2] en 2002 (de tener inquietud, pudiésemos consultar la presentación de Terence TAO[3])—), también es destacable la información proporcionada por Wikipedia[4] y la introducción, en catalán, *Els set problemes del mil·lenni*[5] (si, por ejemplo, tuviésemos un interés especial en la hipótesis de RIEMANN, encuentro recomendable la introducción de Pilar BAYER I ISANT[6] en este último libro —a propósito de la hipótesis de RIEMANN, aún sigue en revisión, que sepamos, la demostración por reducción al absurdo que presentó Michael Francis ATIYAH en el Heidelberg Laureate Forum de 2018[7]—).

Y aún mucho más allá, en general, problemas no resueltos[8] y conjeturas[9].

[1] *Vid.* https://www.claymath.org/millennium-problems.
[2] *Vid. v. gr.* https://en.wikipedia.org/wiki/Grigori_Perelman.
[3] Vid. https://terrytao.wordpress.com/wp-content/uploads/2009/09/poincare.pdf.
[4] *Vid.* https://en.wikipedia.org/wiki/Millennium_Prize_Problems.
[5] *Vid.* https://www.crm.cat/wp-content/uploads/2020/01/7-Problemes.pdf.
[6] *Vid. v. gr.* https://es.wikipedia.org/wiki/Pilar_Bayer_Isant.
[7] *Vid. v. gr.* Sir Michael Francis ATIYAH: *The Riemann Hypothesis (6th HLF – Lecture: Sir Michael Francis Atiyah)*, https://www.youtube.com/watch?v=jXugkzFW5qY; *The Fine Structure Constant*, https://drive.google.com/file/d/1WPsVhtBQmdgQl25_evlGQ1mmTQEoWw4a/view; *The Riemann Hypothesis*, https://drive.google.com/file/d/17NBICP6OcUSucrXKNWvzLmrQpfUrEKuY/view (recordemos que al principio hubo mucho escepticismo [*vid. v. gr.* https://www.science.org/content/article/skepticism-surrounds-renowned-mathematician-s-attempted-proof-160-year-old-hypothesis]).
[8] *Vid. v. gr.* https://en.wikipedia.org/wiki/List_of_unsolved_problems_in_mathematics y https://en.wikipedia.org/wiki/List_of_unsolved_problems_in_computer_science.
[9] *Vid. v. gr.* https://en.wikipedia.org/wiki/List_of_conjectures.

§ A.5 En el entreacto: algo de humor, entretenimiento, curiosidades

- *Piled Higher and Deeper*, (en inglés), <http://phdcomics.com/>.
- *Tim Hunkin and Shane Frazer's The Rudiments of Wisdom Cartoon Encyclopaedia*, (en inglés), <http://www.rudimentsofwisdom.com/default.htm>.
- *Wizards. Abstruse Goose*, (en inglés), <https://abstrusegoose.com/253>.

Apéndice B

Aula de Humanidades Juanelo Turriano (III.ª edición)

> Y mientras las ciencias y las humanidades no puedan hablar y estar en diálogo y avanzar conjuntamente, creo que vamos a seguir atorados en esta falta de comunicación y no vamos a abordar los problemas más importantes de la ciencia, que se tienen que entender de manera humanística. Y también vamos a perder muchas de las preguntas más interesantes que llegan del contexto científico hacia la filosofía.
>
> (Jimena Canales,
> Ciencias y Humanidades deben avanzar de la mano,
> *Aprendemos juntos:* entrevista con Zuberoa Marcos, 20:36[o]).

Nos sumergimos en las humanidades, disciplinas que debiesen acompañar a toda persona científica o ingeniera, como lo serán aquellas a las que en un principio van destinadas estas notas. En su compañía, *part in itinere, part post hoc*, pues ha de leerse mucho, con quietud, para que deje poso.

Su concepción y I.ª edición, inédita, fue fruto del trabajo conjunto con el profesor Andoni Alonso Puelles[1]; en ella nos basamos para construir una II.ª edición que residió en un proyecto de escuela activa[2], apoyo mutuo[3] y aprendizaje libre[4] sobre matemática discreta y numérica en la Wikipedia[5], y en ambas para la presente III.ª edición.

o *Vid.* https://aprendemosjuntos.bbva.com/especial/ciencias-y-humanidades-deben-avanzar-de-la-mano-jimena-canales/.

1 *Vid. v. gr.* https://es.wikipedia.org/wiki/Andoni_Alonso_Puelles.

2 *Vid. v. gr.* https://es.wikipedia.org/wiki/Escuela_activa

3 *Vid. v. gr.* https://es.wikipedia.org/wiki/Apoyo_mutuo

4 Libre en el sentido de Freedomdefined (http://freedomdefined.org/Definition/Es) y en el de *Free Learning* (https://books.google.es/books?id=uiVGEAAAQBAJ).

5 *Vid.* https://es.wikipedia.org/wiki/Wikipedia:Proyecto_educativo/Matemática_discreta_y_numérica.

El Aula de Humanidades Juanelo TURRIANO [6] no tuvo ni tiene el propósito de ofrecer una visión general de las humanidades sino de incidir en temas comunes, como el uso y el impacto recíproco de la ciencia y la tecnología en la sociedad desde el punto de vista humanístico (sin menoscabo del fomento de la lectura y de la interdisciplinariedad subyacentes), esto es, *la convivencialidad de las Humanidades, la Ciencia, la Tecnología, la Sociedad, la Naturaleza y la Innovación,* de modo que la persona científica o ingeniera conozca las demandas y repercusiones éticas y sociales de sus quehaceres, a la vez que disfrute y aprenda del encuentro con las personas autoras de dichas reflexiones y acciones.

Los libros cuya lectura se propone se han clasificado en seis bloques temáticos. Esta estructura permite que la lectura y reflexión sobre cada bloque se lleve a cabo, relajada, que no distraidamente, durante aproximadamente un año. A renglón seguido del último bloque se propone la lectura de algunos más. Tras la lectura de cada libro, quizás no estaría de más que la persona interesada elabore un pequeño resumen del mismo y análisis critico y que busque fuentes documentales con las que contrastar sus conclusiones, a modo de toma de conciencia de lo leído y reflexionado. Asimismo, tras terminar todo un bloque, pudiese hacer algo similar sobre el conjunto.

Existen sesudas selecciones que complementan ésta, como la de Jordi LLOVET I POMAR —*La literatura admirable. Del Génesis a Lolita*, 2018— o la de Nuccio ORDINE —*Classici per la vita. Una piccola biblioteca ideale*, 2016 (*Clásicos para la vida. Una pequeña biblioteca ideal*, 2017)—. En ningún caso debiese quedar restringido el ámbito a los temas mencionados, pues desde el convencimiento de que el es-

[6] Juanelo TURRIANO (Giovanni Torriani o Giannello della Torre) nace en Cremona hacia el 1501 y muere en Toledo el 13 de junio de 1585. En 1529, CARLOS V le nombró relojero real (imperial), asignándole un sueldo de 200 ducados anuales, trabajos extraordinarios aparte. En esta tarea de relojero real destaca como obra cumbre un reloj planetario o astrario, capaz, además de dar las horas y los minutos, de describir las revoluciones de los planetas, con todas sus diferencias, las horas de sol, las horas de luna, aparición de los signos zodiacales …, superando al astrario de DE DONDI (1318-1389), la obra maestra hasta ese momento. Según nos relata Ambrosio DE MORALES, tardó veinte años en concebirlo y tres años y medio en hacerlo. Hizo una réplica de esta máquina, con todas las paredes de cristal, de forma que el «misterio» de su funcionamiento quedase al descubierto. Es conocida como «el cristalino». Sus ayudantes en estas tareas eran Jean VALLIN, relojero de renombre en Flandes, y Jorge DE DIANA. También colaboraba con él Juan DE SEROYAS, relojero y cerrajero de la Corte desde 1561. Ambos construyeron un reloj para el Monasterio del Escorial, que se instaló en 1563.

Tras morir CARLOS V en 1558, aceptó permanecer al servicio de su hijo FELIPE II. Parece ser que pidió aumento de sueldo, que le concedió el rey mediante Cédula Real de 26 de julio de 1562, donde figura el doble de sueldo, aunque también el compromiso de residir en la corte y no hacer más obras que las ordenadas por el rey (pagadas aparte del sueldo).

En su faceta de ingeniero, su obra más famosa, fue una máquina de canjilones en planos inclinados para abastecer de agua del Tajo a Toledo, situada a unos 100 metros sobre el río. Esta máquina es conocida como «el artificio de Juanelo» y es descrita por Ambrosio DE MORALES, cronista de FELIPE II.

El marqués del Vasto le comunica esta empresa en 1565, firmando Turriano ese mismo año una escritura con los representantes de Toledo por la que se compromete a construir un artificio que permita resolver el problema del abastecimiento de agua a la ciudad, hasta esa fecha resuelto a base de subir odres con personas y jumentos. La escritura recogía el compromiso de los representantes de Toledo de pagar la obra con 8000 ducados de oro más una pensión vitalicia de 1900, quince días después de su finalización.

Consiguió de FELIPE II dispensa de no tener que residir en la corte. En 1568 concluyó la construcción del artificio. Éste, que comenzó su funcionamiento el 25 de febrero de 1569, era capaz de subir 17 000 litros diarios —casi 5000 más de lo estipulado que eran «mil seiscientos cántaros de cuatro azumbres»— desde un lugar cercano al puente de Alcántara hasta el Alcázar. Los representantes de Toledo decidieron no pagarle, argumentando que el agua sólo abastecía el real Alcázar. TURRIANO había adelantado más de 8 millones de maravedises, por lo que acudió al rey. En 1573, FELIPE II publicó una cédula para arbitrar el conflicto. Los representantes de la ciudad opinaban que el rey pagase a TURRIANO los 8 millones, que Toledo le pagase 6000 ducados, que TURRIANO construyese un segundo artificio para abastecer la ciudad y que el agua que ésta rindiese fuese propiedad de TURRIANO.

tudio de las humanidades es esencial para entender el mundo, pudiese trabajarse cualquiera de las disciplinas humanísticas.

Tras el encuentro con la persona autora a través de la obra propuesta, no ha de olvidarse explorar, lo más posible, el resto de su obra, para así obtener una visión en conjunto de su pensamiento.

Además del enriquecimiento personal, cultural y humanístico, que conlleva lo anterior, se invita a *compartir lo aprendido y meditado*,

- *contribuyendo a iniciativas del conocimiento libre como Wikipedia* —quizás también en sus wikiproyectos[7]—, Wikilibros, Wikiversidad o cualquiera de los otros proyectos de la fundación Wikimedia; por poner solo un ejemplo, si a fecha de publicación de esta revisión aún no existiese ningún artículo en la Wikipedia en español sobre la obra *El universo abierto* de POPPER (aunque sí que existen sobre *La sociedad abierta y sus enemigos*[8] y sobre *La lógica de la investigación científica* [9]), su lectura y reflexión y la de, por ejemplo, el ensayo del profesor Jorge ESTRELLA, *El universo abierto de Karl Popper* (que aporta una visión global sobre la filosofía de POPPER), podrían servir de base para elaborar dicho artículo;
- *promoviendo encuentros*, presenciales o en línea, para el debate y la discusión, de asistencia y participación libre y gratuita, sobre estos temas.

A continuación, la relación de libros, clasificados por bloques temáticos. Si bien para su lectura pudiese seguirse el orden en que figuran, lo cierto es que la libertad de seguirlo o no, ofrece la flexibilidad, el atractivo y la variedad del encuentro casual. Las indicaciones [∗] designan los pertenecientes a la 1.ª edición del Aula.

A modo de prólogo.

Permítaseme el atrevimiento casi irreverente de recomendar la lectura de la sección

En 1581 terminó el segundo artificio. Pero Toledo tampoco le pagó. Murió arruinado el 13 de junio de 1585. Su nieto se ocupó entonces de mantener los dos artificios hasta su muerte en 1597. A partir de ahí, ambos artificios comenzaron a fallar, hasta que dejaron de funcionar en 1639.

Como dato curioso decir que las columnas del artificio se extrajeron de una de las canteras de granito de Orgaz: «se encuentra la de donde se sacaron los magníficos postes llamados de Juanelo, porque este grande hombre los movía y conducía a Toledo, sin otro auxilio que el de una hija suya, á pesar de que son unas columnas de 75 pies de largo y 5 de diámetro» (Diccionario de Madoz). Cuatro de estas columnas, de 11,50 m de alto por 1,50 m de diámetro, que permanecían en la cantera, fueron trasladadas al Valle de Cuelgamuros (Madrid), durante la construcción del Valle de los Caídos, y allí permanecen.

También se le atribuyen ciertos autómatas: pájaros que podían volar, soldados que simulaban batallas, figuras religiosas con diversos movimientos. Muy famoso fue su «hombre de palo», un muñeco de madera con movilidad propia, del que se dice que era capaz de salir todos los días a la calle, andar hasta el palacio arzobispal y recoger la comida. Debido a ello la calle donde vivió TURRIANO se conoce como calle del hombre de palo.
Por encargo de FELIPE II, escribió *Los veinte y un libros de los ingenios y máquinas de Juanelo*. Algunos historiadores afirman que el pantano de Tibi, atribuido a HERRERA, puede haber sido también obra suya.

Además, TURRIANO era matemático y astrónomo. Por ejemplo, colaboró con GREGORIO XIII en la reforma del calendario juliano.

[7] *Vid.* https://es.wikipedia.org/wiki/Wikipedia:Wikiproyectos.

[8] *Vid.* https://es.wikipedia.org/wiki/La_sociedad_abierta_y_sus_enemigos.

[9] *Vid.* https://es.wikipedia.org/wiki/La_lógica_de_la_investigación_científica.

- «Cooperar es progresar» (págs. 59ss.) de mi artículo «El museo y las arquitecturas de conocimiento libre», *Museos.es*, 7-8: 44–65, 2012 (doi:10.4438/2387-0958-MU-2011-2012-7-8-22) (CC BY 3.0) <https://archive.org/details/LEONROJASJ.M.ElMuseoYLasArquitecturasDeConocimientoLibreMuseos.es2012SEPARATACCBY>.

La transversalidad del conocimiento libre y de la actividad museística como conservadores coadyuvantes del patrimonio humanístico, científico, tecnológico y social me lleva a ello. En este artículo también se discuten las iniciativas WLA y GLAM-Wiki de la Fundación Wikimedia (*vid.* «Ideas de difusión», págs. 50ss.) —más sobre estas iniciativas en Outreach de Wikimedia <https://outreach.wikimedia.org/wiki/GLAM/References#With_reference_to_Wikipedia,_Wikimedia_Commons_or_other_Wikimedia_projects>—.

A modo de ejemplo.

Quizás el más antiguo conocido de tecnología compleja hasta la fecha:

- el mecanismo de Anticitera[10]

(puede verse también, en inglés: *Unlocking the secrets of the world's oldest computer*[11] —Harriet CONSTABLE, 15.07.2021—).

CERO: Filosofía de la Técnica y de la Tecnología.

- Juan David GARCÍA BACCA, *Elogio de la técnica*, 1968.
- Lewis MUMFORD, *Técnica y civilización* (*Technics and Civilization*, 1934), <https://es.wikipedia.org/wiki/Técnica_y_civilización> (reseña).
- Albert BORGMANN, *Technology and the Character of Contemporary Life: A Philosophical Inquiry*, 1984, <https://en.wikipedia.org/wiki/Technology_and_the_Character_of_Contemporary_Life:_A_Philosophical_Inquiry> (reseña).
- Carl MITCHAM, *¿Qué es la filosofía de la tecnología?*, 1989. [*]
- Langdon WINNER, *La ballena y el reactor: una búsqueda de los límites en la era de la alta tecnología* (*The Whale and the Reactor: A Search for Limits in an Age of High Technology*, 1986).
- Alvin TOFFLER, *La tercera ola* (*The Third Wave*, 1980), <https://es.wikipedia.org/wiki/La_tercera_ola> (reseña).
- Jacques ELLUL, *La sociedad tecnológica* (*The Technological Society*, 1954) (en Zenon PYLYSHYN, *Perspectivas de la revolución de los computadores* [*Perspectives on the computer revolution*, 1970]).
- Jürgen HABERMAS, *Ciencia y técnica como ideología* (*Technik und Wissenschaft als "Ideologie"*, 1968).

[10] *Vid. v. gr.* https://es.wikipedia.org/wiki/Mecanismo_de_Anticitera.
[11] *Vid.* https://www.bbc.com/reel/video/p09pcwnz/unlocking-the-secrets-of-the-world-s-oldest-computer.

- Jean Baudrillard, *El sistema de los objetos* (*Le Système des objets*, 1968), <https://es.wikipedia.org/wiki/El_sistema_de_los_objetos> (reseña).
- Gilbert Simondon, *El modo de existencia de los objetos técnicos* (*Du mode d'existence des objets techniques*, 1958), <https://fr.wikipedia.org/wiki/Du_mode_d'existence_des_objets_techniques> (reseña), , <http://www.academia.edu/4184556/Gilbert_Simondon_On_the_Mode_of_Existence_of_Technical_Objects> (texto).
- Herbert Alexander Simon, *Las ciencias de lo artificial* (*The Sciences of the Artificial*, 1969), <https://en.wikipedia.org/wiki/The_Sciences_of_the_Artificial> (reseña).
- Jeremy Rifkin, *El siglo de la biotecnología: el comercio genético y el nacimiento de un mundo feliz* (*The Biotech Century: Harnessing the Gene and Remaking the World*, 1998).
- Ursula Franklin, *El mundo real de la tecnología* (*The Real World of Technology*, 1992).
- Shannon Vallor, *Technology and the Virtues: A Philosophical Guide to a Future Worth Wanting*, 2018.

UNO: Ciencia, Tecnología y Sociedad.

- Guy Debord, *La sociedad del espectáculo* (*La société du spectacle*, 1967), <https://es.wikipedia.org/wiki/La_sociedad_del_espectáculo> (reseña).
- Jorge Luis Borges, *La biblioteca de Babel* (en *Ficciones*, 1944), <https://es.wikipedia.org/wiki/La_biblioteca_de_Babel> (reseña).
- Javier Echeverría, *Introducción a la metodología de la ciencia: la Filosofía de la Ciencia en el siglo XX*, 1989. [∗]
- Andrew Feenberg, *Transformar la tecnología. Una nueva visita a la teoría crítica* (*Transforming Technology: A Critical Theory Revisited*, 2002).
- Karl Popper, *El universo abierto. Una discusión a favor del indeterminismo* (*The Open Universe: An Argument for Indeterminism*, 1956–57 como galeradas inéditas, 1982 como libro). [∗]
- Thomas Kuhn, *¿Qué son las revoluciones científicas? y otros ensayos* (1989) (*What are scientific revolutions?*, 1981; *Commensurabillity, comparability, communicability*, 1982; *Rationality and theory choice*, 1983). [∗]
- Simone Weil, *Sobre la ciencia* (*Sur la science*, 1966).
- Charles Fort, *El libro de los condenados* (*The Book of the Damned*, 1919), <https://es.wikipedia.org/wiki/El_libro_de_los_condenados> (reseña), <https://es.wikisource.org/wiki/en:The_Book_of_the_Damned> (texto).
- Zygmunt Bauman, *Comunidad. En busca de seguridad en un mundo hostil* (*Community. Seeking Safety in an Insecure World*, 2001).

- Cathy O'Neil, *Armas de destrucción matemática: cómo el big data aumenta la desigualdad y amenaza la democracia* (2017) (*Weapons of Math Destruction. How Big Data Increases Inequality and Threatens Democracy*, 2016), <https://es.wikipedia.org/wiki/Armas_de_destrucción_matemática> (reseña).
- Nuccio Ordine, *La utilidad de lo inútil* (*L'utilità dell'inutile*, 2013).
- Donald A. Norman, *El diseño de los objetos del futuro. La interacción entre el hombre y la máquina* (*The design of future things*, 2007).
- Kevin Kelly, *Lo inevitable* (*The Inevitable*, 2016), <https://en.wikipedia.org/wiki/The_Inevitable_(book)> (reseña).
- Donna Haraway, *Un manifiesto cíborg* (*A Cyborg Manifesto*, 1985), <https://es.wikipedia.org/wiki/El_Manifiesto_Cyborg> (reseña).

DOS: Imagen del Ser Humano.

- José Ortega y Gasset, *La rebelión de las masas*, 1930, <https://es.wikipedia.org/wiki/La_rebelión_de_las_masas> (reseña).
- —, *Meditación de la técnica*, 1939.
- George H. Mead, *Espíritu, persona y sociedad* (*Mind, Self and Society*, 1934, <https://en.wikipedia.org/wiki/Mind,_Self_and_Society> (reseña).
- John R. Searle, *El misterio de la conciencia* (*The Mystery of Conciousness*, 1997). [*]
- Roger Penrose, *Las sombras de la mente: hacia una comprensión científica de la consciencia* (*Shadows of the Mind: A Search for the Missing Science of Consciousness*, 1994), <https://es.wikipedia.org/wiki/Las_sombras_de_la_mente> (reseña). [*]
- Alan Ross Anderson (*ed.*), *Controversia sobre mentes y máquinas* (*Minds and Machines*, 1964). [*]
- Bart Kosko, *Pensamiento borroso. La nueva ciencia de la lógica borrosa* (*Fuzzy Thinking. The New Science of Fuzzy Logic*, 1993). [*]
- Paul Virilio, *El cibermundo, la política de lo peor: entrevista con Philippe Petit* (*Cybermonde, la politique du pire : entretien avec Philippe Petit*, 1996).
- Edward Ashford Lee, *Plato and the Nerd: The Creative Partnership of Humans and Technology*, 2017.
- Adam Smith, *Teoría de los sentimientos morales* (*The Theory of Moral Sentiments*, 1759), <https://es.wikipedia.org/wiki/Teoría_de_los_sentimientos_morales> (reseña), <https://en.wikipedia.org/wiki/s:The_Theory_of_Moral_Sentiments> (texto).
- Hannah Arendt, *La condición humana* (*The Human Condition*, 1958), <https://en.wikipedia.org/wiki/The_Human_Condition_(book)> (reseña). [*]

- Simone de Beauvoir, *El segundo sexo* (*Le Deuxième Sexe*, 1949), <https://es.wikipedia.org/wiki/El_segundo_sexo> (reseña).
- Luce Irigaray, *Espéculo de la otra mujer* (*Speculum. De l'autre femme*, 1974).
- Luc Ferry, *Aprender a vivir: Filosofía para mentes jóvenes* (*Apprendre à vivre : Traité de philosophie à l'usage des jeunes générations*, 2006).

TRES: Multiculturalismo y Globalización.

- Iván Illich, *La Convivencialidad* (*Tools for Conviviality*, 1973), <https://en.wikipedia.org/wiki/-Tools_for_Conviviality> (reseña). [∗]
- Peter Sloterdijk, *Normas para el parque humano. Una respuesta a la Carta sobre el humanismo de Heidegger* (*Regeln für den Menschenpark. Ein Antwortschreiben zu Heideggers Brief über den Humanismus*, 1999). [∗]
- Hans Küng, *Una ética mundial para la economía y la política* (*Weltethos fur Weltpolitik und Weltwirtschaft*, 1997). [∗]
- Robert Nozick, *Anarquía, Estado y utopía* (*Anarchy, State, and Utopia*, 1974), <https://es.wikipedia.org/wiki/Anarquía,_Estado_y_utopía> (reseña).
- Donaldo Macedo, Bessie Dendrinos y Panayota Gounari, *Lengua, ideología y poder. La hegemonía del inglés* (*The Hegemony of English*, 2003).
- William Foote Whyte, *La sociedad de las esquinas* (*Street Corner Society*, 1943), <https://en.wikipedia.org/wiki/Street_Corner_Society> (reseña).
- Jorge Riechmann, *Un mundo vulnerable. Ensayos sobre ecología, ética y tecnociencia* (2000). [∗]
- Edgar Morin, *La vía. Para el futuro de la humanidad* (*La Voie. Pour l'avenir de l'humanité*, 2011).
- Christian Laval y Pierre Dardot, *La nueva razón del mundo. Ensayo sobre la sociedad neoliberal* (*La nouvelle raison du monde*, 2009).
- —, *Común. Ensayo sobre la revolución en el siglo XXI* (*Commun, Essai sur la révolution au XXIe siècle*, 2014).
- Serge Latouche, *La apuesta por el decrecimiento: ¿cómo salir del imaginario dominante?* (*Le pari de la décroissance*, 2006).
- Paul Bloom, *Contra la empatía: argumentos para una compasión racional* (*Against empathy: The case for rational compassion*, 2016).
- Michel Onfray, *Política del rebelde. Tratado de la resistencia y la insumisión* (*Politique du rebelle : Traité de résistance et d'insoumission*, 1997).

- Lawrence G. Lovasik, *El poder oculto de la amabilidad* (*The Hidden Power of Kindness: A Practical Handbook for Souls Who Dare to Transform the World, One Deed at a Time*, 1962).

CUATRO: Ética y Valor Humano.

- Francisco Díez de Velasco Abellán, *Hombres, ritos, Dioses. Introducción a la historia de las religiones*, 1995. [∗]
- Jean-Jacques Rousseau, *El contrato social; o los principios del derecho político* (*Du contrat social; ou Principes du droit politique*, 1762), <https://es.wikipedia.org/wiki/El_contrato_social> (reseña). [∗]
- Martin Heidegger, *La pregunta por la técnica* (*Die Frage nach der Technik*, 1954), <https://revistafilosofia.uchile.cl/index.php/RDF/article/view/45002> (texto). [∗]
- Max Weber, *La ética protestante y el espíritu del capitalismo* (*Die protestantische Ethik und der 'Geist' des Kapitalismus*, 1904–1905), <https://es.wikipedia.org/wiki/La_ética_protestante_y_el_espíritu_del_capitalismo> (reseña). [∗]
- Ayn Rand, *La rebelión de Atlas* (*Atlas Shrugged*, 1957), <https://es.wikipedia.org/wiki/La_rebelión_de_Atlas> (reseña).
- Joseph Conrad, *El corazón de las tinieblas* (*Heart of Darkness*, 1899), <https://es.wikipedia.org/wiki/El_corazón_de_las_tinieblas> (reseña). [∗]
- Cesare Beccaria, *De los delitos y las penas* (*Dei delitti e delle pene*, 1764), <https://es.wikipedia.org/wiki/De_los_delitos_y_las_penas> (reseña).
- Christian Laval, *La escuela no es una empresa: el ataque neoliberal a la enseñanza pública* (*L'école n'est pas une entreprise: Le néo-libéralisme à l'assaut de l'enseignement public*, 2003).
- Martha Nussbaum, *Sin fines de lucro: por qué la democracia necesita de las humanidades* (*Not for profit: why democracy needs the humanities*, 2010).
- Sigmund Freud, *El malestar en la cultura* (*Das Unbehagen in der Kultur*, 1930), <https://es.wikipedia.org/wiki/El_malestar_en_la_cultura> (reseña). [∗]
- Lev Tolstoi, *Confesión* (*Ispoved*, 1884), <https://en.wikipedia.org/wiki/A_Confession> (reseña), <https://en.wikipedia.org/wiki/s:A_Confession_(Tolstoy)> (texto).
- Francis Collins, *¿Cómo habla Dios? La evidencia científica de la fe* (*The Language of God: A Scientist Presents Evidence for Belief*, 2006), <https://en.wikipedia.org/wiki/The_Language_of_God> (reseña).
- John Stuart Mill, *Sobre la libertad* (*On liberty*, 1859), <https://es.wikipedia.org/wiki/Sobre_la_libertad> (reseña).
- Frédéric Gros, *Desobedecer* (*Désobéir*, París: Albin Michel, 2017).

CINCO: Evolución.

- George ORWELL, *1984* (*Nineteen eighty-four*, 1949), <https://es.wikipedia.org/wiki/1984_(novela)> (reseña).
- Aldous HUXLEY, *Un mundo feliz* (*Brave New World*, 1932), <https://es.wikipedia.org/wiki/Un_mundo_feliz> (reseña).
- —, *Nueva visita a un mundo feliz* (*Brave New World Revisited*, 1958), <https://es.wikipedia.org/wiki/Nueva_visita_a_un_mundo_feliz> (reseña).
- Daniel DENNETT, *La peligrosa idea de Darwin: la evolución y los significados de la vida* (*Darwin's Dangerous Idea: Evolution and the Meanings of Life*, 1996), <https://en.wikipedia.org/wiki/Darwin's_Dangerous_Idea> (reseña). [∗]
- George BASSALLA, *La evolución de la tecnología* (*The Evolution of Technology*, 1988). [∗]
- Paul FEYERABEND, *Contra el método: esquema de una teoría anarquista del conocimiento* (*Against Method: Outline of an Anarchist Theory of Knowledge*, 1970/1975), <https://es.wikipedia.org/wiki/Contra_el_método> (reseña), <http://mcps.umn.edu/philosophy/completeVol4.html> (texto). [∗]
- Hans JONAS, *El principio de responsabilidad* (*Das Prinzip Verantwortung*, 1979), <https://es.wikipedia.org/wiki/El_principio_de_responsabilidad> (reseña). [∗]
- Herman MELVILLE, *Moby Dick; o La Ballena* (*Moby-Dick; or, The Whale*, 1851), <https://es.wikipedia.org/wiki/Moby-Dick> (reseña).
- Yuval Noah HARARI, *Sapiens: De animales a dioses: Una breve historia de la humanidad* (*Sapiens: A Brief History of Humankind*, 2014), <https://es.wikipedia.org/wiki/Sapiens:_De_animales_a_dioses> (reseña).
- —, *Homo Deus: Breve historia del mañana* (*Homo Deus: A Brief History of Tomorrow*, 2016), <https://es.wikipedia.org/wiki/Homo_Deus:_Breve_historia_del_mañana> (reseña).
- Hernán ZIN, *La libertad del compromiso: cambiar tu vida para cambiar el mundo* (2005).
- Paola CAVALIERI y Peter SINGER, *El Proyecto «Gran Simio»: la igualdad más allá de la humanidad* (*The Great Ape Project: Equality Beyond Humanity*, 1993). [∗]
- Steven M. WISE, *Sacudiendo la jaula: Hacia los Derechos de los animales* (*Rattling the Cage: Toward Legal Rights for Animals*, 2000), <https://lawcommons.lclark.edu/cgi/viewcontent.cgi?article=1387&context=alr> (reseña), <https://atlasofthefuture.org/es/project/nonhuman-rights-project/> (*Nonhuman Rights Project*).

- Samuel BUTLER, *Erewhon, un mundo sin máquinas* (*Erewhon: or, Over the Range*, 1872), <https://en.wikipedia.org/wiki/Erewhon> (reseña), <http://nzetc.victoria.ac.nz/tm/scholarly/tei-ButErew.html> (texto). [*]

A continuación.

- Baruch SPINOZA, *Ética* (*Ethica ordine geometrico demonstrata*, 1677), <https://es.wikipedia.org/wiki/Ética_(Spinoza)> (reseña), <https://es.wikisource.org/wiki/en:Ethics_(Spinoza)> (texto).
- Thomas HOBBES, *Leviatán, o La materia, forma y poder de una república eclesiástica y civil* (*Leviathan, or The Matter, Forme and Power of a Common-Wealth Ecclesiasticall and Civil*, 1651), <https://es.wikipedia.org/wiki/Leviatán_(Hobbes)> (reseña), <https://es.wikisource.org/wiki/en:Leviathan> (texto).
- Arthur SCHOPENHAUER, *El mundo como voluntad y representación* (*Die Welt als Wille und Vorstellung*, 1819), <https://es.wikipedia.org/wiki/El_mundo_como_voluntad_y_representación> (reseña).

Y para no finalizar.

- Henry PETROSKI, *La ingeniería es humana. La importancia del fallo en el éxito del diseño*, 2007, <https://www.cinter.es/laingenieriaeshumana_prologo.htm> (fragmentos del prólogo).
- Jesús Pedro ZAMORA BONILLA,*Sacando consecuencias: una filosofía para el siglo XXI*, 2017, <https://revistas.usc.gal/index.php/agora/article/view/5021/5436> (reseña).
- Antonio DIÉGUEZ LUCENA,*Pensar la tecnología. Una guía para comprender filosóficamente el desarrollo tecnológico actual*, 2024, <https://www.jotdown.es/2025/08/antonio-dieguez-entrevista/> (entrevista).

Anexo

Me identifico en el lenguaje, pero sólo perdiéndome en él como un objeto. Lo que se realiza en mi historia no es el pretérito-definido de lo que fue, puesto que ya no es, ni siquiera el perfecto de lo que ha sido en lo que yo soy, sino el futuro anterior de lo que yo habré sido para lo que estoy llegando a ser.

(Jacques Lacan, *Escritos 1* [226] [p. 288]).

Las trampas de Circe

Este anexo lleva por título el inicio del libro póstumo *Las trampas de Circe: falacias lógicas y argumentación informal* [125] de Montserrat BORDES SOLANAS (Barcelona, 1965-2010) —profesora de Bioética, de Lógica y de Filosofía de la Ciencia, entre otras materias—, en su honor.

Aquí me limito a reproducir el índice de su *taxonomía de falacias* (la numeración corresponde a los capítulos y subcapítulos de su libro). Lo hago desde mi admiración por el trabajo de la autora; espero despertar la curiosidad en quienes lean, asimismo como que dicha reproducción contribuya a que se hagan una idea del enorme esfuerzo que le supuso esta sistematización.

Sin más sobre el particular, por ahora, sólo resta mi recomendación por el estudio profundo, reflexivo y sosegado de su obra.

5 Falacias formales

- 5.1 Falacia del hombre enmascarado o falacia epistémica.
- 5.2 Falacia del medio no distribuido.
- 5.3 Falacias del condicional.
  - Falacia por afirmación del consecuente.
  - Falacia por negación del antecedente.
- 5.4 Falacias modales. La falacia de Hume.
- 5.5 Falacias probabilísticas.
  - 5.5.1 Falacia del jugador o de la lotería.
  - 5.5.2 Falacia de la conjunción.
- 5.6 Falacia *ad logicam* (falacia de la falacia).

6 Falacias informales que contravienen el criterio de claridad.

Epílogo

> *Le meilleur remède aux turbulences de l'esprit, c'est d'apprendre. C'est la seule chose qui ne se détériore jamais. On peut vieillir et trembler, au sens anatomique du terme ; on peut veiller la nuit en écoutant le désordre de ses veines ; on peut perdre son unique amour et voir s'évanouir sa fortune par la faute d'un monstre ; on peut contempler le monde autour de soi dévasté par des fous dangereux, ou savoir que son honneur est piétiné dans les égouts des esprits les plus vils. Dans de telles conditions, il n'y a qu'une seule chose à faire : apprendre.* [El mejor remedio para la turbulencia de la mente es aprender. Es la única cosa que nunca sale mal. Uno puede envejecer y temblar, en un sentido anatómico; uno puede quedarse despierto por la noche escuchando el desorden de sus venas; uno puede perder el único amor y ver su fortuna desmayarse a causa de un monstruo; uno puede mirar el mundo a tu alrededor devastado por lunáticos peligrosos, o sabiendo que su honor es pisoteado en las alcantarillas de las mentes más viles. En estas condiciones, sólo queda una cosa por hacer: aprender.]
>
> (Marguerite YOURCENAR, *Sources II*, Gallimard, 1999).

> *Wir müssen wissen—wir werden wissen* [Debemos saber y sabremos].
>
> (David HILBERT).

Confío en que hayamos conseguido atravesar algunas de las puertas iniciales de la matemática discreta que se han ido entreabriendo. Ha sido de sumo agrado poner todo mi empeño en que lo logremos.

Mas, ¡ay, qué mucho queda por conocer hasta atisbar los márgenes de lo recóndito, de las profundidades, de lo difícil!

Sin embargo, más allá, lo recóndito, profundo, difícil; entrar en tales lares, queda fuera del contexto de estas notas.

Muchas gracias por su tiempo, comprensión y paciencia. Mis mejores deseos les acompañan.

Referencias y referentes

Lo que en los libros no está, la vida te lo enseñará.

(SEVILLA y ZURDO [34]).

Aquí están los textos que me han inspirado la exposición de la materia (algunos ya recogidos en sus contextos de referencia, al final de los diferentes capítulos de estas notas). No están todos, algunos que no he recogido aquí aparecen en diversas notas a pie de página. Sea como sea, ni siquiera éstos junto a aquéllos constituyen una lista exhaustiva de textos relevantes en referencia a lo tratado en estas notas, sino más bien una muestra representativa de lo por mí leído, aunque sin duda sí que es un punto de inicio para búsquedas y encuentros multimodales. Quizás algún día esta lista se asemeje a una bibliografía anotada, por ahora baste con la información contextual en cada una de sus citas.

Apostillar que el tiempo transcurrido desde que brotaron estos textos no es excusa para su abandono, pues no les resta nada de actualidad. En la práctica, cuando lleguemos a uno de ellos desde un ejemplo o actividad, estudiemos los demás ejemplos, ejercicios o problemas relacionados que resuelva o proponga dicho texto. Apliquemos lo mismo a las llegadas desde la parte «teórica». Nos será muy de provecho.

Toda bibliografía participa del efecto descenso infinito, de la iteración en la navegación, de la hipertextualidad: una bibliografía lleva a otra y ésta a otra, y así sucesivamente. No tengamos miedo a conocer (*cfr. v. gr.* BOGHOSSIAN [227]).

[0] Juan de VALDÉS. *Diálogo de la lengua*. Ediciones Cátedra, Madrid, Comunidad de Madrid (ES-M), España, 13.ª ed., 2018. ix

[1] Juan Miguel LEÓN-ROJAS. *Juicios por comparación, inferencias lingüísticas y actos de decisión en sistemas de representación de conocimiento efectivamente computables basados en unidades vagamente perfiladas*. Tesis Doctoral, Departamento de Informática, Área de Lenguajes y Sistemas Informáticos, Cáceres, Extremadura (ES-EX), España, 2003. Cerrada el 1 de julio de 2003, leída el 9 de enero de 2004 y publicada en junio de 2005 en CD-ROM por el Servicio de Publicaciones de la Universidad de Extremadura, ISBN: 84-7723-648-8. (Esta versión 0.0 está disponible, p. ej., en: https://archive.org/details/jmLeonRojas-TESIS-v0.0). xvi, 82, 184, 510, 520, 521, 638

[2] Douglas Richard HOFSTADTER. *Gödel, Escher, Bach: un eterno y grácil bucle*. Tusquets Editores, Barcelona, Cataluña (ES-CT), España, 1987. Traducido por Alejandro LÓPEZ ROUSSEAU y Mario Arnaldo USABIAGA BANDIZZI de *Gödel, Escher, Bach: an Eternal Golden Braid (GEB)*, Nueva York, Basic Books, 1979. xx, 185

[3] John Rogers SEARLE. *Actos de habla*. Planeta-De Agostini, Barcelona, Cataluña [ES-CT], España, 1994. xlvii

[4] Carl E. LINDERHOLM. *Mathematics made difficult*. World Pub, Nueva York, Nueva York (US-NY), Estados Unidos de América, 1972. li

[5] CC2020 Task FORCE. *Computing Curricula 2020: Paradigms for Global Computing Education*. Association for Computing Machinery, New York, NY, USA, 2020. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2020.pdf. lii

[6] CE2016 Steering COMMITTEE. *Computer Engineering Curricula 2016: Curriculum Guidelines for Undergraduate Degree Programs in Computer Engineering*. Association for Computing Machinery, New York, NY, USA, 2016. https://www.acm.org/binaries/content/assets/education/ce2016-final-report.pdf. lii

[7] Joint Task Force ON COMPUTING CURRICULA, Association FOR COMPUTING MACHINERY (ACM) y IEEE Computer SOCIETY. *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. Association for Computing Machinery, New York, NY, USA, 2013. https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf. lii

[8] Alfs BERTZISS. A mathematically focused curriculum for computer science. *Communications of the ACM*, 30:356–365, 1987. lii

[9] Silverio LANZA. *Cuentos escogidos*. Asociación de Escritores y Artistas, Madrid, Comunidad de Madrid (ES-M), España, 1908. lvii

[10] Silverio LANZA. El paletismo. *Alma Española*, II(11):7–8, 1904. lvii

[11] Rafael RODRÍGUEZ VIDAL. *Diversiones matemáticas*. Reverté, Barcelona, Cataluña (ES-CT), España, 1984. lvii

[12] Francisco RUBIALES MORENO. *Políticos, los nuevos amos: rebeldía ciudadana frente a la democracia degenerada*. Almuzara, 1. ed ed., 2007. lix

[13] Manuel SIERRA FRANCO. *¿Por qué los humanos somos así?* Editorial Castalia, Madrid, Comunidad de Madrid [ES-M], España, 2005. lix

[14] Nicholas RESCHER. *Los límites de la ciencia*. Tecnos, 1994. lx

[15] M. X y Santiago TARÍN. *Viaje por las mentiras de la historia universal: compendio de mentiras, tópicos, mitos y leyendas de la historia en el cine, la literatura y el saber oficial*. Documentos. Belacqva, 3.ª ed., 2006. lx

[16] Jean Pierre ASTOLFI. *El "error" un medio para enseñar: Gaston Bachelard, Jean Piaget*. Díada, 1999. lxi

[17] Elena SANZ. Equivocarse es de sabios, 2022. lxi

[18] Antoine HOULOU-GARCIA. *Mathematikós: Vidas y hallazgos de los matemáticos de Grecia y Roma*. El Libro de bolsillo. Alianza, Madrid, Comunidad de Madrid (ES-M), España, 2021. lxi

[19] Raúl IBÁÑEZ TORRES. La invasión de los ladrones de matemáticas: matemáticas en la vida cotidiana. En: *Ciencia200607*. Caja de Burgos, Burgos, España, 2007. lxv

[20] Juan Miguel LEÓN ROJAS. Liberalidad del conocimiento desde la cesión de derechos de propiedad intelectual. En: Dirección General de Sociedad de la Información JUNTA DE EXTREMADURA (ed.), *Encuentro Internacional sobre Conocimiento Libre*, páginas 190–200. Junta de Extremadura (Consejería de Infraestructuras y Desarrollo Tecnológico), Mérida, Extremadura (ES-EX), España, 2005. https://archive.org/details/LenRojasJ.M.2005liberalidadDelConocimientoDesdeLaCesinDe (accedido el 26.1.2024). ©(de esta edición facsimilar) CC BY 4.0. lxviii

[21] Juan Miguel LEÓN ROJAS. Sobre la liberalidad de la ciencia y la liberación del científico. *Epistemowikia*, 0, 2007. Disponible en: https://archive.org/details/SobreLaLiberalidadDeLaCienciaYLaLiberacionDelCientifico. lxviii

[22] Juan Miguel LEÓN ROJAS. Y lo que te rondaré, Commonledge. *Argumentos de Razón Técnica*, 10, 2007. Disponible en: https://archive.org/details/leon-rojas-j.-m.-2007-y-lo-que-te-rondare-commonledge-argumentos-de-razon-tecnica-10-cap.-7. lxviii

[23] Juan Miguel LEÓN ROJAS. El museo y las arquitecturas de conocimiento libre. *Museos.es*, 7-8:44–65, 2012. Disponible en: https://archive.org/details/LEONROJASJ.M.ElMuseoYLasArquitecturasDeConocimientoLibreMuseos.es2012SEPARATACCBY. lxviii

[24] VARIOS. Sage Math Español. https://www.sagemath.org/es/ (accedido el 26.1.2024). ©CC BY-NC-SA. cii, ciii

[25] Ana María VIEITES RODRÍGUEZ, Felicidad AGUADO MARTÍN, Felipe GAGO COUSO, Manuel LADRA GONZÁLEZ, Gilberto PÉREZ VEGA y Concepción VIDAL MARTÍN. *Teoría de grafos. Ejercicios resueltos y propuestos. Laboratorio con Sage*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2014. http://www.paraninfo.es/catalogo/9788428337076/teoria-de-grafos–ejercicios-y-problemas-resueltos. ©TDR. cii, ciii

[26] SAGE DEVELOPMENT TEAM. *Sage Documentation v10.1*, 2023. https://doc.sagemath.org/html/en/index.html (accedido el 26.1.2024). ©gratis OA. cii, civ

[27] Paul ZIMMERMANN, Alexandre CASAMAYOU, Nathann COHEN, Guillaume CONNAN, Thierry DUMONT, Laurent FOUSSE, François MALTEY, Matthias MEULIEN, Marc MEZZAROBBA, Clément PERNET, Nicolas M. THIÉRY, Erik BRAY, John CREMONA, Marcelo FORETS, Alexandru GHITZA y Hugh Thomas THOMAS. *Computational Mathematics with SageMath*. Autoedición, Nancy, Francia, 2018. Ediciones en alemán, francés e inglés. https://www.sagemath.org/sagebook/english.html (accedido el 26.1.2024). ©CC BY-SA. cii, civ

[28] Francisco Javier GONZÁLEZ ORTIZ. Proyecto MATEX, 2004. http://personales.unican.es/gonzaleof/ (accedido el 25.1.2018). ©gratis OA. ciii

[29] TEXTOS MAREA VERDE. Apuntes Marea Verde, 2024. http://www.apuntesmareaverde.org.es/grupos/mat/index.html (accedido el 26.1.2024). ©CC BY-NC-SA. ciii

[30] CK-12 FOUNDATION. K-12 FlexBooks, 2024. https://www.ck12.org/fbbrowse/ (accedido el 26.1.2024). ©CK-12 License. ciii

[31] SIYAVULA EDUCATION. Open Textbooks, 2024. https://www.siyavulaeducation.com/work-oer.html (accedido el 26.1.2024). ©CC BY-ND. ciii

[32] Félix GARCÍA MERAYO. *Matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 2015. ciii, 588, 688, 714, 1119, 1421

[33] Juan Antonio Nicolás y María José Frápolli. *Teorías de la verdad en el siglo XX*. Semilla y surco Serie de sociología. Tecnos, Madrid, Comunidad de Madrid [ES-M], España, 1997. 1

[34] Julia Sevilla Muñoz y María I. Teresa Zurdo Ruiz-Ayúcar (Dirs.). *Refranero multilingüe*. Instituto Cervantes (Centro Virtual Cervantes), Madrid, Comunidad de Madrid (ES-M), España, 2010. https://cvc.cervantes.es/lengua/refranero/ (accedido el 26.1.2024). ©gratis OA. 1, 15, 109, 1462, 1474

[35] Peter Pin-Shan Chen. The entity-relationship model—toward a unified view of data. *ACM Transactions on Database Systems*, 1(1):9–36, Mar 1976. 34

[36] Igor T. Hawryszkiewycz. *Introducción al análisis y diseño de sistemas con ejemplos prácticos*. Anaya Multimedia, 1990. 34

[37] Julio Fernández Ostolaza y Álvaro Moreno Bergareche. *Vida artificial*. Eudema Biología. Eudema, 1992. 35

[38] Graciela Reyes. *El abecé de la pragmática*. Cuadernos de lengua espanola. Arco Libros, Madrid, 10.ª ed., 2017. 44, 48, 95

[39] Ann Hutchinson. *Labanotation: the system of analyzing and recording movement*. Routledge/Theatre Arts Books, 3.ª ed., rev. ed., 1991. 47

[40] John Florian Sowa. *Knowledge Representation. Logical, Philosophical, and Computational Foundations*. Brooks/Cole, Pacific Grove, California, 2000. 48, 60

[41] Hilary Putnam. *El pragmatismo: un debate abierto*. Serie CLADEMA. Gedisa, 1.ª ed., 1999. 48

[42] Joaquín Carreras Artau. *Introducción a la filosofía (lógica, psicología y ética)*. Alma Mater, Barcelona, Cataluña (ES-CT), España, 4.ª ed., 1944. 60

[43] Antonio Aróstegui Megías. *Curso de concienciación filosófica*. Marsiega, Madrid, Comunidad de Madrid (ES-M), España, 1977. 60

[44] Esther Torrego. Temas de gramática y cognición: primeras y segundas lenguas. En: Natalia Catalá, José A. Díez Calzada y Manuel García-Carpintero (ed.), *El lenguaje y la mente humana*, Ariel filosofía, capítulo 4, páginas 121–141. Ariel, Barcelona, Cataluña (ES-CT), España, 1.ª ed., 2002. 63

[45] Beatriz Sanz Alonso. La negación en español. En: Mercedes Rueda Rueda, Elena Prado Ibán, Janick Le Men Loyer y Francisco Javier Grande Alija (ed.), *Tendencias actuales en la enseñanza del español como lengua extranjera II (Actas del VI Congreso Internacional de ASELE [1995])*, páginas 379–384. Secretariado de Publicaciones de la Universidad de León, León, Castilla y León (ES-CL), España, 1996. https://cvc.cervantes.es/ensenanza/biblioteca_ele/asele/asele_vi.htm (accedido el 26.1.2024). ©gratisOA. 80

[46] Marisa Santiago Barriendos, Fernando Polanco Martínez y Pedro Gras Manzano. «No veo que lo entiendas». La no aserción. Propuesta didáctica del modo verbal en oraciones sustantivas. En: María Auxiliadora Castillo Carballo, Olga Cruz Moya, Juan Manuel García Platero y Juan Pablo Mora Gutiérrez (ed.), *Las gramáticas y los diccionarios en la enseñanza del español como segunda lengua: deseo y realidad (Actas del XV Congreso Internacional de ASELE [2004])*, páginas 824–830. Secretariado de Publicaciones de la Universidad de Sevilla, Sevilla, Andalucía (ES-AN), España, 2005. https://cvc.cervantes.es/ensenanza/biblioteca_ele/asele/asele_xv.htm (accedido el 26.1.2024). ©gratisOA. 82

[47] Carlos Díaz. *La buena aventura del comunicarse*. Nossa y Jara, Madrid, Comunidad de Madrid (ES-M), España, 1995. 83

[48] Tomás Labrador Gutiérrez. Funciones o valores –gramaticales o semánticos– de los elementos de enlace. En: Salvador Montesa Peydró y Antonio Garrido Moraga (ed.), *Actas del III Congreso Nacional de ASELE (1991). El español como lengua extranjera: de la teoría al aula*, páginas 327–342. ASELE, Málaga, Andalucía (ES-AN), España, 1993. https://cvc.cervantes.es/ensenanza/biblioteca_ele/asele/asele_iii.htm (accedido el 26.1.2024). ©gratisOA. 84

[49] John Cleveland Cooley. *A Primer of Formal Logic*. MacMillan, Nueva York, Nueva York (US-NY), Estados Unidos de América, 1942. ©TDR. 84

[50] Jean Piaget y Rolando García (Eds.). *Hacia una Lógica de Significaciones*. Bibliotecas Universitarias. Centro Editor de América Latina, 1988. (Traducción al español de: <Vers une logique des significations>, Ginebra, Murionde, 1987). 91

[51] Fernando Lázaro Carreter y Vicente Tusón Valls. *Curso de lengua española*. Anaya, Madrid, Comunidad de Madrid (ES-M), España, 1981. 94, 175

[52] Judea Pearl. *Causality: Models, Reasoning and Inference*. Cambridge University Press, Cambridge, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 2.a ed., 2009. ©TDR. 95

[53] Judea Pearl y Dana Mackenzie. *The Book of Why: The New Science of Cause and Effect*. Penguin,

Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 2019. ©TDR. 95

[54] Chiara Marletto. *The Science of Can and Can't: A Physicist's Journey Through the Land of Counterfactuals*. Allen Lane, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 2021. ©TDR. 95

[55] Edsger Wybe Dijkstra. *A Discipline of Programming*. Prentice Hall, Englewood Cliffs, Nueva Jersey (US-NJ), Estados Unidos de América, 1976. ©TDR. 113

[56] David Gries. *The Science of Programming*. Monographs in Computer Science. Springer-Verlag, Nueva York, Nueva York (US-NY), Estados Unidos de América, 1981. ©TDR. 113, 698

[57] Willard Van Orman Quine. *Mathematical Logic*. Harvard University Press, Cambridge, Massachusetts (US-MA), Estados Unidos de América, 2.ª ed., 1981. ©TDR. 124

[58] Scientific Development Corporation (SDC). *MINIVAC 601. Book III: How Computers Make Logical Decisions*. SDC, Watertown, Middlesex, Mancomunidad de Massachusetts (US-MA), Estados Unidos de América, 1961. 128

[59] Antony J. Crilly. *50 cosas que hay que saber sobre matemáticas*. Ariel, Barcelona, Cataluña (ES-CT), España, 2009. 130, 134

[60] Herbert Bruce Enderton. *A mathematical introduction to logic*. Harcourt/Academic Press, San Diego, Condado de San Diego, California (US-CA), Estados Unidos de América, 2.ª ed., 2001. 159, 174, 254, 362, 395, 438, 460, 492

[61] Michael Huth y Mark Ryan. *Logic in Computer Science: Modelling and Reasoning about Systems*. Cambridge University Press, Cambridge, Massachusetts (US-MA), Estados Unidos de América, 2004. ©TDR. 171

[62] María Manzano Arjona y Antonia Huertas Sánchez. *Lógica para principiantes*. Filosofía y Pensamiento. Alianza Editorial, S. A., Humanes de Madrid, Comunidad de Madrid [ES-M], España, 2004. 174, 254, 314, 362, 394, 395, 437, 459, 491

[63] Pascual Casañ Muñoz y Amador Antón Antón. *Lógica matemática. Ejercicios. I. Lógica de enunciados*. NAU llibres, Valencia, España, 1991. 174, 254, 362

[64] Manuel Garrido Giménez. *Lógica simbólica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1.ª ed., 1977. (8.ª reimpresión, 1989). 174, 254, 362, 363, 394, 395, 402, 403, 413, 438, 445, 452, 456, 457, 459, 491, 588

[65] Carmen García Trevijano. *El arte de la lógica*. Serie de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1999. 174, 254, 362, 394, 438, 459, 491

[66] Manuel Garrido Giménez, Luis Manuel Valdés Villanueva, Jesús Mosterín de las Heras, Alfonso García Suárez y Carlos-Peregrín Fernández Otero. *Lógica y lenguaje*. Cuadernos de filosofía y ensayo. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 1989. 174, 254, 362, 395, 438, 459, 492

[67] Raymond Merrill Smullyan. *First-Order Logic*. Dover Publications, Inc., Nueva York, NY, EUA, 1995. (Republicación corregida de la edición publicada por Springer-Verlag en 1968). 174, 254, 274, 362, 363, 395, 438, 459, 492

[68] Emilio Alarcos Llorach. *Gramática estructural (según la escuela de Copenhague y con especial atención a la lengua española)*. Biblioteca románica hispánica. Gredos, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1984. 175

[69] Francisco Marcos Marín. *Aproximación a la gramática española*. Colección Didaxis. Cincel, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1975. 175

[70] Peter Cathcart Wason y Philip Nicholas Johnson-Laird. *Psychology of Reasoning: Structure and Content*. Harvard University Press, Cambridge, Massachusetts, USA, 1972. 184

[71] Russell Revlin, Von Otto Leirer, Hallie Kay Yopp y Ruth Helen Yopp. The belief-bias effect in formal reasoning: The influence of knowledge on logic. *Memory and Cognition*, 8(6):584–592, 1980. 184

[72] Raymond S. Nickerson, David N. Perkins y Edward E. Smith. *The Teaching of Thinking*. Lawrence Erlbaum Associates, Hillsdale, New Jersey, USA, 1985. 184

[73] Bruno Latour. *Ciencia en Acción. Cómo Seguir a los Científicos e Ingenieros a Través de la Sociedad*. Labor, Barcelona, España, 1992. (Traducido por Eduardo Aibar, Roberto Méndez y Estela Ponisio de: <Science in Action: How to Follow Scientists and Engineers Through Society>, Open University Press, Buckingham, 1987). 184

[74] Alexander Romanovich Luria. *Cognitive Development: Its Cultural and Social Foundations*. Harvard University Press, Cambridge, MA, USA, 1976. 184

[75] Michael Cole y Sylvia Scribner. *Culture and Thought: A Psychological Introduction*. Wiley, New York, NY, USA, 1974. 184

[76] Alfred North WHITEHEAD y Bertrand Arthur William RUSSELL. *Principia Mathematica*. Cambridge University Press, Cambridge, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1910. Vol. I (http://name.umdl.umich.edu/AAT3201.0001.001), Vol. II (http://name.umdl.umich.edu/AAT3201.0002.001) y Vol. III (http://name.umdl.umich.edu/AAT3201.0003.001) (accedido el 26.1.2024). ©Dominio Público. 184

[77] David HILBERT y Wilhelm Friedrich ACKERMANN. *Elementos de lógica teórica*. Estructura y función. Tecnos, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1993. 184

[78] Jan ŁUKASIEWICZ. *Elements of Mathematical Logic*. Macmillan, Nueva York, Nueva York (US-NY), Estados Unidos de América, 1963. ©TDR. 184

[79] Stephen Cole KLEENE. *Introduction to Metamathematics*. P. Noordhoff N.V., Groninga, Provincia de Groninga (GR), Países Bajos, 1952. 184

[80] Gerhard GENTZEN. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39, 1935. I. (DOI: 10.1007/BF01201353) (pp. 176–210) (http://gdz.sub.uni-goettingen.de/dms/resolveppn/?PPN=GDZPPN002375508) y II. (10.1007/BF01201363) (pp. 405–431) (http://gdz.sub.uni-goettingen.de/dms/resolveppn/?PPN=GDZPPN002375605) (accedidos el 26.1.2024). ©TDR. 185, 190, 408

[81] Stanisław JAŚKOWSKI. *On the Rules of Suppositions in Formal Logic*. Studia Logica. Nakładem Seminarjum Filozoficznego Wydziału Matematyczno-Przyrodniczego Uniwersytetu Warszawskiego, 1934. 185, 190, 408

[82] Jesús MOSTERÍN DE LAS HERAS. *Lógica de primer orden*. Ariel, 1983. 189

[83] Martin GARDNER. *Entertaining Mathematical Puzzles*. Dover Publications, Nueva York, Nueva York (US-NY), Estados Unidos de América, 1986. ©TDR. 234

[84] Raymond Merrill SMULLYAN. *What is the name of this book?–The Riddle of Dracula and Other Logical Puzzles*. Prentice-Hall, Englewood Cliffs, Nueva Jersey (US-NJ), Estados Unidos de América, 1978. ©TDR. 234

[85] Raymond Merrill SMULLYAN. *¿Cómo se llama este libro?* Cátedra, Madrid, Comunidad de Madrid (ES-M), España, 18.ª ed., 2011. ©TDR. 234, 249, 251

[86] Alexandr Vladimirovich ZHÚKOV, Peter Isaak SAMOVOL y Mark Vilen APPLEBAUM. *La matemática elegante. Problemas y soluciones detalladas*. Matematnka. URSS, Moscú, 2007. 234, 477, 478

[87] Raymond Merrill SMULLYAN. *Juegos por siempre misteriosos*. Gedisa, Barcelona, Cataluña (ES-CT), España, 2.ª ed., 1995. Traducción de Margarita MIZRAJI. ©TDR. 250

[88] Roland Carl BACKHOUSE. *Program construction and verification*. Prentice-Hall International, Englewood Cliffs, Nueva Jersey (US-NJ), Estados Unidos de América, 1986. ©TDR. 251

[89] Frank Markham BROWN. *Boolean Reasoning: The Logic of Boolean Equations*. Dover Publications, Mineola, Nueva York (US-NY), Estados Unidos de América, 2.ª ed., 2012 (reimp.). ©gratisOA. 257

[90] Evert Willem BETH. *The Foundations of Mathematics. A Study in the Philosophy of Science*. North-Holland, Amsterdam, Países Bajos, 1959. 274, 363, 395

[91] Kaarlo Jaakko Juhani HINTIKKA. *The Philosophy of Mathematics*. Oxford, 1969. 274, 363, 395

[92] Wilfrid HODGES. *Logic: an introduction to elementary logic*. Penguin, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1991. 312

[93] Dave BARKER-PLUMMER, Jon BARWISE, John ETCHEMENDY, Albert LIU, Michael MURRAY y Emma PEASE. *Language, proof, and logic*. CSLI Publ, Stanford, California, EE. UU., 2.ª ed., 2011. 323

[94] Ernest LEPORE y Sam CUMMING. *Meaning and argument: an introduction to logic through language*. Wiley-Blackwell, Chichester, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 2.ª ed., 2009. 326

[95] Hanne Riis NIELSON y Flemming NIELSON. *Semantics with applications: an appetizer*. Undergraduate topics in computer science. Springer, 2007. 361

[96] Rafael BENEYTO TORRES. Laberintos analíticos. *Teorema: Revista internacional de filosofía*, 1(4):19–30, 1971. 363, 395

[97] Kaarlo Jaakko Juhani HINTIKKA. Form and content in quantification theory. *Acta Philosophica Finnica*, 8:57–55, 1955. 363, 395

[98] Richard Carl JEFFREY. *Formal Logic: its Scope and Limits*. McGraw-Hill, 1967. 363, 396

[99] Amador ANTÓN ANTÓN y Pascual CASAÑ MUÑOZ. *Lógica matemática. II. Lógica de predicados*. NAU llibres, Valencia, España, 1998. 394, 395, 438, 459, 491

[100] Robin SMITH. Aristotle's Logic. En: Edward Nouri ZALTA (ed.), *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, fall ed., 2020. https://plato.stanford.edu/archives/fall2020/entries/aristotle-logic/. 400

[101] Henrik LAGERLUND. Medieval Theories of the Syllogism. En: Edward N. ZALTA (ed.), *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Summer 2021 ed., 2021. 400

[102] Max BLACK. I.-The identity of indiscernibles. *Mind*, LXI(242):153–164, 1952. 407

[103] Alfredo DEAÑO. *Introducción a la lógica formal*. Alianza, Madrid, Comunidad de Madrid (ES-M), España, 2002. 414

[104] Susan HAACK. *Deviant Logic*. Cambridge University Press, Cambridge, UK, 1974. (Lógica Divergente, Paraninfo, Madrid, Comunidad de Madrid [ES-M], España, 1980). 423

[105] Deborah Jo BENNETT. *Logic Made Easy: How to Know when Language Deceives You*. Penguin Books, Londres, 2005. 432

[106] Walter BRENNER, Rüdiger ZARNEKOW y Hartmut WITTIG. *Intelligent Software Agents*. Springer Berlín Heidelberg, 1998. 437

[107] John Alan ROBINSON. A Machine-Oriented Logic Based on the Resolution Principle. *Journal of the ACM*, 12(1):23–41, January 1965. 448

[108] Kurt GÖDEL. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatshefte für Mathematik und Physik*, 37(1):349–360, December 1930. 452

[109] Leon HENKIN. The completeness of the first-order functional calculus. *Journal of Symbolic Logic*, 14(3):159–166, September 1949. 452

[110] Gisbert HASENJAEGER. Über ω-Unvollständigkeit in der Peano-Arithmetik. *Journal of Symbolic Logic*, 17(2):81–97, June 1952. 452

[111] Leopold LÖWENHEIM. Über Möglichkeiten im Relativkalkül. *Mathematische Annalen*, 76(4):447–470, December 1915. 456

[112] Alonzo CHURCH. An Unsolvable Problem of Elementary Number Theory. *American Journal of Mathematics*, 58(2):345, Abr 1936. 457, 530

[113] Alan Mathison TURING. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, s2-42(1):230–265, 1937. 457

[114] Paul Isaac BERNAYS y Moses Ilyich SCHÖNFINKEL. Zum Entscheidungsproblem der mathematischen Logik. *Mathematische Annalen*, 99(1):342–372, December 1928. 457

[115] George POLYA. *How to Solve It: A New Aspect of Mathematical Method*. Princeton University Press, Princeton, New Jersey, USA, primera ed., 1945. 463

[116] William Nathan SCHOENFELD. *Teoría de los programas de reforzamiento*. Trillas, México, 1979. 464

[117] Philip J. DAVIS y Reuben HERSH. *Experiencia matematica*. Labor, Barcelona, Cataluña (ES-CT), España, 1989. 464

[118] John MASON, Leone BURTON y Kaye STACEY. *Pensar matemáticamente*. Labor, Barcelona, Cataluña (ES-CT), España, 1989. 464

[119] Miguel de GUZMÁN OZAMIZ. *El rincón de la pizarra. Ensayos de visualización en análisis matemático. Elementos básicos del análisis*. Ciencia Hoy. Pirámide, Madrid, Comunidad de Madrid [ES-M], España, 2001. 473

[120] Thomas TYMOCZKO. The Four-Color Problem and its Philosophical Significance. *Journal of Philosophy*, 76(2):57–83, 1979. 488

[121] Philip J. DAVIS y Reuben HERSH. *Experiencia Matemática*. Ministerio de Educación y Ciencia - Ed. Labor, Madrid (Comunidad de Madrid [ES-M]) - Barcelona, España, 1989. 489

[122] Richard HAMMACK. *Book of proof*. Hammack, Richmond, Virginia, EE. UU., 3.ª ed., 2022. 491, 808, 811, 813, 830

[123] George PÓLYA. *Cómo plantear y resolver problemas*. Matemáticas. Trillas, Ciudad de México (MX-CMX), Estados Unidos Mexicanos, reimp. ed., 2008. 491

[124] Jiří MATOUŠEK y Jaroslav NEŠETŘIL. *Invitación a la matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2008. 491, 589, 688, 714, 1148, 1288, 1401, 1408, 1422

[125] Montserrat BORDES SOLANAS. *Las trampas de Circe: falacias lógicas y argumentación informal*. Colección Teorema. Serie Mayor. Cátedra, 3.ª ed., 2017. 496, 1454

[126] Jesús MOSTERÍN DE LAS HERAS. *Los Lógicos*. Espasa Calpe, Madrid, Comunidad de Madrid [ES-M], España, 2000. 511

[127] Iván GUZMÁN DE ROJAS. *Logical and Linguistic Problems of Social Communication with the Aymara People*. International Development Research Centre (IDRC), Ottawa, Canadá, 1984. (Disponible en: http://www.aymara.org/biblio/igr/igr.html). 516

[128] Lorenzo PEÑA. Lógicas multivalentes. En: *Lógica (Enciclopedia Iberoamericana de Filosofía, Vol. 7)*. Trotta & Consejo Superior de Investigaciones Científicas (CSIC), 1995. 516, 517

[129] Nicholas RESCHER. *Many-valued Logic*. McGraw-Hill, New York, NY, USA, 1969. 517

[130] José FERRATER MORA. *Diccionario de Filosofía (4 tomos)*. Ariel (Grupo Planeta), Barcelona, España, 1994. 517

[131] José FERRATER MORA y Hugues LEBLANC. *Lógica Matemática*. Fondo de Cultura Económica, México, 1975. 517

[132] Emil Leon POST. Introduction to a general theory of elementary propositions of logic. *American Journal of Mathematics*, 43:163–185, 1921. 517

[133] Stephen Cole KLEENE. On notation for ordinal numbers. *The Journal of Symbolic Logic*, 3(4):150–155, 1938. 517

[134] Stephen Cole KLEENE. *Introduction to Metamathematics*. Van Nostrand Co., Inc., New York, NY, USA, 1952. (*Introducción a la Metamatemática*, Tecnos, Madrid, Comunidad de Madrid [ES-M], España, 1974). 517

[135] Dmitry Anatol'evich BOCHVAR. On a three-valued logical calculus and its application to the analysis of the classical extended functional calculus. *History and Philosophy of Logic*, 24:87–112, 1981. (Traducido al inglés de: Od odnom tréhznačnom isčislénii i égo priménénii k analizu paradoksov klassićéskogo rassirénnogo funkcional'nogo isćislenija. *Matématičéskij Sbornik*, 4:287-308, 1939). 517

[136] Arend HEYTING. *Intuitionism: An Introduction*. North Holland, Amsterdam, Nederland, 1956. 517

[137] Hans REICHENBACH. *Philosophic Foundations of Quantum Mechanics*. Universityof California, Berkeley, 1944, 1965. 517

[138] M. WAJSBERG. Aksjomatyzacja trójwartościowego rachunku zdań. *Comptes rendus de la Société des Sciences et des Lettres de Varsovie*, Cl. III(24):126–148, 1931. 517

[139] George Jiří KLIR y Bo YUAN. *Fuzzy Sets and Fuzzy Logic. Theory and Applications*. Prentice Hall, Upper Saddle River, Nueva Jersey (US-NJ), Estados Unidos de América, 1995. 521, 540

[140] Máximo ANZOLA GONZÁLEZ y José Ramón CARUNCHO CASTRO. *Problemas de álgebra. Tomo 1: Conjuntos - Grupos*. Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1981. ©TDR. 546, 564, 571, 588, 688, 710, 712, 713, 746, 748, 750, 853, 855, 857, 930, 933, 935, 936, 940

[141] John Kenneth TRUSS. *Discrete mathematics for computer scientists*. Addison-Wesley, Bungay, Suffolk (GB-SFK), Reino Unido, 1991. 554, 558, 572, 588, 688, 713, 714

[142] José Antonio ALONSO JIMÉNEZ, Joaquín BORREGO DÍAZ, Mario de Jesús PÉREZ JIMÉNEZ y José Luis RUIZ REINA. *Curso Práctico de Teoría de Conjuntos*. La Ñ, Sevilla, Andalucía (ES-AN), España, 1998. 567, 588, 628, 688, 714, 751, 753, 783

[143] Calixto BADESA, Ignacio JANÉ y Ramón JANSANA. *Elementos de lógica formal*. Ariel Filosofía, Barcelona, Cataluña (ES-CT), España, 1998. 567

[144] Agustín de la VILLA CUENCA. *Problemas de Álgebra (con esquemas teóricos)*. CLAGSA, Madrid, Comunidad de Madrid (ES-M), España, 4.ª ed., 2010. ©TDR. 571, 572, 588, 688, 713, 940

[145] José GARCÍA GARCÍA y Manuel LÓPEZ PELLICER. *Álgebra lineal y geometría: curso teórico-práctico*. Marfil, Alcoy, Hoya de Alcoy, Alicante (ES-A), España, 8.ª ed., 1992. 587, 687, 713, 940

[146] Armando Óscar ROJO. *Álgebra I*. El Ateneo, Buenos Aires (AR-C), Argentina, 1986. ©TDR. 587, 635, 687, 713, 940

[147] Herbert Bruce ENDERTON. *Elements of Set Theory*. Academic Press, Londres, Gran Londres, Inglaterra (GB-ENG), Reino Unido de Gran Bretaña e Irlanda del Norte, 1977. 587, 687, 713, 750, 803, 830

[148] Karel HRBACEK y Thomas J. JECH. *Introduction to set theory*. Monographs and textbooks in pure and applied mathematics. Marcel Dekker, Nueva York, Nueva York (US-NY), Estados Unidos de América, 3.ª ed., 1999. 587, 713, 750, 783, 803

[149] Józef Maria BOCHEŃSKI. *Compendio de lógica matemática*. Colección Lógica y Teoría de la Ciencia. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1982. Traducido del inglés *A Précis of Mathematical Logic* (1959), traducido a su vez de *Précis de logique mathématique* (1948), Bussum, North Holland: F. G. Kroonder. 588, 606, 687, 713

[150] Félix GARCÍA MERAYO, Gregorio HERNÁNDEZ PEÑALVER y Antonio NEVOT LUNA. *Problemas resueltos de matemática discreta*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 2018. 588, 634, 688, 714, 993, 1050, 1055, 1074, 1076, 1120, 1264, 1265, 1289, 1354, 1357, 1422

[151] Kenneth Howard ROSEN. *Matemática discreta y sus aplicaciones*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 5.ª ed., 2004. (La 5.ª edición es la última en español). 588, 688, 714, 805, 807, 811, 827, 828, 830, 1288, 1422

[152] Kenneth Howard ROSEN. *Discrete Mathematics and its Applications*. McGraw-Hill, Nueva York, Nueva York (US-NY), Estados Unidos de América, 7.ª ed., 2012. 588, 688, 714, 828, 830, 1422

[153] Francisco José GONZÁLEZ GUTIÉRREZ. *Apuntes de Matemática Discreta*. El autor, Cádiz, Andalucía (ES-AN), España, 2004. 588, 688, 714, 1017, 1018, 1029, 1085, 1096, 1104, 1105, 1119

[154] Carlos GARCÍA GÓMEZ, Josep María LÓPEZ BESORA y Dolors PUIGJANER RIBA. *Matemática discreta*. Pearson Educación, Madrid, Comunidad de Madrid (ES-M), España, 2002. 589, 688, 714, 1101, 1105, 1120, 1289, 1422

[155] Ralph Peter GRIMALDI. *Matemáticas discreta y combinatoria*. Addison-Wesley Iberoamericana, Wilmington, New Castle, Delaware (US-DE), Estados Unidos de América, 3.ª ed., 1997. 589, 688, 714, 1119, 1289, 1366, 1422

[156] Juan Carlos FERRANDO PÉREZ y Valentín GREGORI GREGORI. *Matemática discreta*. Reverté, Barcelona, Cataluña (ES-CT), España, 2.ª ed., 2012. 589, 688, 714, 1228, 1230, 1231, 1276, 1289, 1422

[157] Kenneth Allen ROSS y Charles Richard Bowers WRIGHT. *Matemáticas discretas*. Prentice-Hall Hispanoamericana, Naucalpan de Juárez, Estado Libre y Soberano de México (MX-MEX), Estados Unidos Mexicanos, 2.ª ed., 1990. 589, 689, 714, 1278, 1289, 1422

[158] Richard JOHNSONBAUGH. *Discrete Mathematics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 8.ª ed., 2018. 589, 689, 714, 1289, 1341, 1345, 1407, 1410, 1422

[159] George BOOLOS. *Logic, Logic, and Logic*. Harvard University Press, Cambridge, Massachusetts, Estados Unidos, 1998. 606

[160] Ramón JANSANA. *Una Introducción a la Lógica Modal*. Tecnos, Madrid, Comunidad de Madrid [ES-M], España, 1990. 623, 664

[161] Sixto RÍOS INSÚA, María Concepción BIELZA LOZOYA y Alfonso MATEOS CABALLERO. *Fundamentos de los Sistemas de Ayuda a la Decisión*. Ra-Ma, Madrid, Comunidad de Madrid [ES-M], España, 2002. 623, 664

[162] Jesús MOSTERÍN DE LAS HERAS. *Conceptos y Teorías en la Ciencia*. Alianza, Madrid, Comunidad de Madrid [ES-M], España, 1984. 623, 625

[163] Arnold KAUFMANN, Thierry DUBOIS y Michel COOLS. *Exercises avec Solutions sur la Théorie des Sous-Ensembles Flous*. Masson et Cie, París, Francia, 1975. (Tradución al español por Fernando Ibarra Aispuro: <Ejercicios con soluciones sobre la teoría de los subconjuntos borrosos>, Cia. Editorial Continental S. A. de C. V., México, 1982). 638

[164] María Purificación GALINDO VILLARDÓN. *Estudio Crítico de Ordenaciones*. Universidad Nacional a Distancia, 1981. (Trabajo para optar al grado de Licenciado dirigido por el Prf. Dr. Norberto Cuesta Dutari). 644, 645

[165] Karl MENGER. *Kurventheorie*. Teubner, Leipzig, Germany, 1932. (Chelsea Pub Co, 2nd edition, february 1968). 644

[166] Norberto CUESTA DUTARI. *La Sinfonía del Infinito*. Universidad de Salamanca, Salamanca, España, 1981. 645

[167] Roger Newland SHEPARD. The analysis of proximities: Multidimensional scaling with an unknown distance function. I. *Psychometrika*, 27(2):125–140, June 1962. 646

[168] Roger Newland SHEPARD. The analysis of proximities: Multidimensional scaling with an unknown distance function. II. *Psychometrika*, 27(3):219–246, September 1962. 646

[169] Joseph Bernard KRUSKAL. Multidimensional scaling by optimizing goodness of fit to a nonmetric hypothesis. *Psychometrika*, 29(1):1–27, March 1964. 646

[170] Joseph Bernard KRUSKAL. Nonmetric multidimensional scaling: A numerical method. *Psychometrika*, 29(2):115–129, June 1964. 646

[171] John Somerset CHIPMAN. The foundations of utility. *Econometrica*, 28(2):193–224, 1960. (Reimpreso en: Readings in Mathematical Psychology, Vol. II, edited by R. Duncan Luce, Robert R. Bush and Eugene Galanter, New York: John Wiley & Sons, Inc., 1965, pp. 419-450). 664

[172] Douglas John WHITE. *Teoría de la Decisión*. Alianza, Madrid, Comunidad de Madrid [ES-M], España, segunda ed., 1979. (Traducción al español de José Luis García Molina de: <Decision Theory>, George Allen and Unwin, London, 1969). 664

[173] María Carmen ESCRIBANO RÓDENAS. Las relaciones de orden en la modernización de las preferencias. Resolución de modelos con la Teoría de Decisión Multicriterio. En: Paula CORCHO SÁNCHEZ (ed.), *La Utilización de las Matemáticas en la Economía del Año 2000*, páginas 41–57. Universidad de Extremadura. Servicio de Publicaciones, Cáceres, España, 2001. 664

[174] Vladimir ESTIVILL-CASTRO y Derick WOOD. A new measure of presortedness. *Information and Computation*, 83(1):111–119, 1989. (Disponible en: https://core.ac.uk/download/pdf/82003055.pdf). 671

[175] Vladimir ESTIVILL-CASTRO y Derick WOOD. A survey of adaptive sorting algorithms. *ACM Computing Surveys (CSUR)*, 24(4):441–476, 1992. (Disponible en: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.45.8017). 671

[176] Miguel CÓRDOBA BUENO. *La Toma de decisiones en la práctica*. Delta Publicaciones Universitarias, 2005. 676, 677, 678, 687

[177] George Jiří KLIR, Ute H. ST. CLAIR y Bo YUAN. *Fuzzy set theory: foundations and applications*.

Prentice Hall, Upper Saddle River, Nueva Jersey (US-NJ), Estados Unidos de América, 1997. 680, 687

[178] Wayne D. BLIZARD. Multiset Theory. *Notre Dame Journal of Formal Logic*, 30(1):44, 1989. https://projecteuclid.org/download/pdf_1/euclid.ndjfl/1093634995. 705

[179] Richard JOHNSONBAUGH. A Discrete Intermediate Value Theorem. *The College Mathematics Journal*, 29(1):42–42, Jan 1998. Disponible en: https://www.maa.org/sites/default/files/0746834259610.di020780.02p0372v.pdf, en las *Classroom Capsules and Notes* (https://www.maa.org/node/1231827/classroom-capsules-and-notes) de la MAA (Mathematical Association of America). 706, 708

[180] Julius Wilhelm Richard DEDEKIND. *Was sind und was sollen die Zahlen? / von Richard Dedekind*. Vieweg, 1888. 724

[181] Geoffrey HUNTER. *Metalógica. Introducción a la metateoría de la lógica clásica de primer orden*. Colección Lógica y Teoria de la Ciencia. Paraninfo, Madrid, 1981. 725

[182] Francesc ROSSELL I PUJÓS. *El infinito. ¿Es un viaje o un destino?* Grandes ideas de las matemáticas. EMSE EDAPP y Prisanoticias Colecciones, Barcelona, Cataluña (ES-CT), España, 2019. 750, 783

[183] Julián GARRIDO GARRIDO. *Verdad matemática: introducción a los fundamentos de la matemática*. Ciencia abierta. Nivola, Madrid, Comunidad de Madrid (ES-M), España, 2003. 750, 783

[184] Azriel LEVY. *Basic Set Theory*. Perspectives in Mathematical Logic Series. Springer-Verlag, Berlin - Heidelberg - New York, 1979. 753, 783

[185] Keith James DEVLIN. *Fundamentals of Contemporary Set Theory*. Springer - Verlag, New York - Heidelberg - Berlin, 1979. 753, 783

[186] Gaisi TAKEUTI y Wilson Miles ZARING. *Introduction to Axiomatic Set Theory*. Springer - Verlag, New York - Heidelberg - Berlin, 1971. 753, 783

[187] Paul HALMOS. *Naive set theory*. Van Nostrand Company, Princeton, NNew Jersey (US-NJ), Estados Unidos, 1960. 753

[188] Carlos IVORRA CASTILLO. *Lógica y teoría de conjuntos*. Autoedición, Valencia, Comunidad Valenciana [ES-VC], España, 2022. https://www.uv.es/ivorra/Libros/Logica.pdf (accedido el 26.1.2024). ©gratisOA. 783

[189] Carlos IVORRA CASTILLO. *Álgebra*. Autoedición, Valencia, Comunidad Valenciana [ES-VC], España, 2022. https://www.uv.es/ivorra/Libros/Al.pdf (accedido el 26.1.2024). ©gratisOA. 803

[190] James BRADLEY. *Introduction to discrete mathematics*. Addison-Wesley, Reading, Middlesex, Mancomunidad de Massachusetts (US-MA), Estados Unidos de América, 1988. 827, 830, 1289, 1407, 1410, 1422

[191] Brian HOPKINS. *Resources for Teaching Discrete Mathematics: Classroom Projects, History Modules, and Articles*. The Mathematical Association of America, Washington (US-WA), Estados Unidos de América, 2009. 828

[192] Leandro PARDO LLORENTE, Ángel FELIPE ORTEGA y Julio Ángel PARDO LLORENTE. *Programación lineal entera: aplicaciones prácticas en la empresa*. Díaz de Santos, Madrid, Comunidad de Madrid [ES-M], España, 1990. 871

[193] Garrett BIRKHOFF. *Lattice Theory*. Colloquium Publications, 25. American Mathematical Society, Providence, RI, USA, 1948. 923

[194] George GRÄTZER. *General Lattice Theory*. Birkhäuser Verlag, Basel, Stuttgart, 1978. 923

[195] Jean DESANTI. Observaciones sobre la conexión de las nociones de génesis y estructura en matemáticas. En: *Las Nociones de Estructura y Génesis, tomo II: Matemática y Biología*. Nueva Visión, Buenos Aires, Argentina, 1975. 924

[196] Jesús IBÁÑEZ (COORD.). *Nuevos Avances en la Investigación Social II: La Investigación Social de Segundo Orden*. Proyecto A Ediciones. Kings Tree S. L., Barcelona, España, 1998. 924

[197] Máximo ANZOLA GONZÁLEZ y José Ramón CARUNCHO CASTRO. *Problemas de álgebra. Tomo 2: Anillos - Polinomios - Ecuaciones.* Los autores, Madrid, Comunidad de Madrid (ES-M), España, 3.ª ed., 1982. ©TDR. 934, 936, 940, 994, 996, 1059, 1078, 1079, 1083, 1102, 1120

[198] Alexei Ivanovich KOSTRIKIN. *Introducción al álgebra*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 2.ª ed., 1992. ©TDR. 940

[199] Alain BIGARD, Maurice CRESTEY y Jacques GRAPPY. *Problemas de álgebra moderna*. Reverté, Barcelona, Cataluña (ES-CT), España, 1975. ©TDR. 940

[200] Carlos MUNUERA GÓMEZ y Juan Gabriel TENA AYUSO. *Codificación de la información*. Secretariado de Publicaciones e Intercambio Científico de la Universidad de Valladolid, Valladolid, Campiña del Pisuerga, Castilla y León (ES-CL), España, 1997. ©TDR. 940

[201] Thomas William JUDSON y Robert Arnold BEEZER. *Abstract Algebra: Theory and Applications*. Autoedición, Nacogdoches, Condado de Nacogdoches, Texas (US-TX), Estados Unidos de América, 2022. http://abstract.ups.edu/sage-aata.html. ©GFDL. 941

[202] GAP SUPPORT GROUP. *GAP Documentation*, 2024. https://www.gap-system.org/Doc/-doc.html (accedido el 26.1.2024). ©gratis OA. 941

[203] Alexander HULPKE. *Using GAP*, 2000. https://www.math.colostate.edu/~hulpke/-paper/gap4tut.pdf (accedido el 26.1.2024). ©gratis OA. 941

[204] Johannes KÜSTER. Math never seen. *TUGboat: Communications of the TEX Users Group*, 31(2):228–229, 2010. 968, 978

[205] María Dolores de PRADA VICENTE y Ricardo RODRÍGUEZ RODRÍGUEZ. *Cómo enseñar la divisibilidad*. Anaya, Madrid, Comunidad de Madrid (ES-M), España, 1982. 970, 1101, 1119

[206] Javier REVUELTA y Vicente PONSODA. *Simulación de modelos estadísticos en ciencias sociales*. La Muralla - Hespérides, Madrid (Comunidad de Madrid [ES-M], España) - Salamanca, España, 2003. 1006

[207] Lorenzo ABELLANAS RAPÚN y Alberto GALINDO TIXAIRE. *Teoría y problemas de métodos de cálculo*. McGraw-Hill, Madrid, Comunidad de Madrid (ES-M), España, 1992. 1022

[208] Yákov Isidórovich PERELMÁN. *Álgebra recreativa*. Mir, Moscú (RU-MOW), Distrito federal Central, Federación de Rusia, 1.ª ed., 1965. (7.ª reimpresión, 1989). (Traducido del ruso al español por C. Pérez y F. Petrov). 1099, 1104, 1120

[209] Emiliana OLIVÁN CALZADA. Ecuaciones diofánticas. *PublicacionesDidácticas*, 26:51–62, junio 2012. 1104, 1120

[210] Wenceslao CIURÓ I SUREDA. *Juegos de manos de sobremesa*. Artes Gráficas C. I. O., Madrid, Comunidad de Madrid [ES-M], España, 1961. (El padre Wenceslao también era conocido por su alias: Ling-Kai-Fu). 1106, 1107

[211] Marco MEIROVITZ y Paul I. JACOBS. *Desafíe a su inteligencia*. Martínez Roca, Barcelona, Cataluña (ES-CT), España, 1985. 1106

[212] Walter MORA-FLORES. *Introducción a la teoría de números. Ejemplos y algoritmos*. Instituto Tecnológico de Costa Rica, Cartago, Cantón de Cartago, Provincia de Cartago (CR-C), República de Costa Rica, 2010. hhttps://hdl.handle.net/2238/6299. ©CC BY-NC-ND. 1119

[213] Felicidad AGUADO MARTÍN, Felipe GAGO COUSO, Manuel LADRA GONZÁLEZ, Gilberto PÉREZ VEGA, Concepción VIDAL MARTÍN y Ana María VIEITES RODRÍGUEZ. *Problemas resueltos de Combinatoria. Laboratorio con SageMath*. Paraninfo, Madrid, Comunidad de Madrid (ES-M), España, 2018. 1120, 1289, 1334, 1337, 1423

[214] José Ramón FRANCO BRAÑAS, María Candelaria ESPINEL FEBLES y Pedro Ramón ALMEIDA BENÍTEZ. *Manual de combinatoria*. Dirección General de Universidades e Investigación del Gobierno de Canarias, La Laguna - Tenerife, Canarias (ES-CN), España, 2005. 1137, 1139, 1143, 1147, 1184, 1275, 1277, 1289, 1422

[215] Giridhar TALLA. Why solve a problem twice? Design patterns let you apply existing solutions to your code. *The Overflow*, 2021. The Stack Overflow Network. Disponible en Internet: https://stackoverflow.blog/2021/10/13/why-solve-a-problem-twice-design-patterns-let-you-apply-existing-solutions-to-your-code/. 1190

[216] Jean-Guy DUBOIS. Une systématique des configurations combinatoires simples. *Educational Studies in Mathematics*, 15:37–57, 1984. DOI:10.1007/BF00380438. 1190, 1288

[217] Richard Anthony BRUALDI. *Introductory Combinatorics*. Pearson Education, Hoboken, Hudson, Nueva Jersey (US-NJ), Estados Unidos de América, 5.ª ed., 2010. 1243, 1289, 1422

[218] Peter Jephson CAMERON. *Notes on combinatorics*. Autopublicación, 2013. 1250, 1289, 1422

[219] Kenneth Paul BOGART. *Combinatorics throuhg guided discovery*. Autopublicación, 2004. 1273, 1276, 1289, 1422

[220] María del Carmen BATANERO BERNABÉU, Virginia NAVARRO-PELAYO y Juan DÍAZ GODINO. *Razonamiento combinatorio*. Síntesis, Madrid, Comunidad de Madrid (ES-M), España, 1994. 1288

[221] Jesús de la CAL AGUADO. El problema de la ruina del jugador. *SIGMA. Revista de Matemáticas*, 29:109–119, 2006. 1407

[222] Mykel J. KOCHENDERFER, Tim A. WHEELER y Kyle H. WRAY. *Algorithms for Decision Making*. The MIT Press, Cambridge, Massachusetts, Estados Unidos, 2022. http://algorithms-book.com/files/dm.pdf (accedido el 19.1.2026). ©CC BY-NC-ND. 1440

[223] Pascal MICHEL. The Busy Beaver Competition: a historical survey. *arXiv*, página 0906.3749, 2022. 1440

[224] *The Electronic Journal of Combinatorics*, 2024. http://www.combinatorics.org/ojs/index.php/eljc/index (accedido el 26.1.2024). ©gratis OA. 1440

[225] Terry TAO. *What's new*, 2024. blog de Terence Tao, Mozart of maths. https://terrytao.wordpress.com/ (accedido el 26.1.2024). ©gratis OA. 1440

[226] Jacques LACAN. *Escritos 1*. Psicología y psicoanálisis. Siglo XXI, México, 3.ª ed., 2009. 1453

[227] Paul A. BOGHOSSIAN. *El miedo al conocimiento: contra el relativismo y el constructivismo*. Alianza, Madrid, Comunidad de Madrid (ES-M), España, 2009. 1462

[228] Alan DAVIDSON. logicproof - Box proofs for propositional and predicate logic, 2014. https://ctan.org/pkg/logicproof (accedido el 26.1.2024). ©LPPL. 1494

[229] Peter SMITH. Logic Matters, 2024. https://www.logicmatters.net (accedido el 26.1.2024). ©gratis OA. 1494

Índice de nombres y materias

Quien deja camino y toma vereda piensa que adelanta, pero rodea.
(José María Sbarbi y Osuna. (1922 = 1943): *Gran diccionario de refranes de la lengua española*. Madrid, 1922. Edición consultada: Joaquín Gil Editor. Buenos Aires, 1943. [Vía [34]]).

Este índice recoge en sus entradas, en orden alfabético, algunas de las personas y materias que aparecen en el cuerpo de la obra. Los números tras cada entrada remiten a algunas de las páginas en las que aparece la persona o la materia referida.
Que nos disculpen quienes sientan falta.
De las materias, igual.
O que nos culpen. Serenidad y paciencia. ¡¡Incompleto, por ahora!!. Sea como fuere están en la obra (ya se buscaron y encontraron, por eso notaron su ausencia).

Que este índice no reprima nuestra curiosidad.
El conocimiento está en el cuerpo de la obra:
quien explore, halle.

B

Manuscribamos

Reflexiones, análisis, analogías, estudios, intereses, acciones, mapas, críticas y ampliaciones ineludibles.

Entintemos la página.

Manuscribamos

Reflexiones, análisis, analogías, estudios, intereses, acciones, mapas, críticas y ampliaciones ineludibles.

Entintemos la página.

Manuscribamos

Reflexiones, análisis, analogías, estudios, intereses, acciones, mapas, críticas y ampliaciones ineludibles.

Entintemos la página.

Manuscribamos

Reflexiones, análisis, analogías, estudios, intereses, acciones, mapas, críticas y ampliaciones ineludibles.

Entintemos la página.

Manuscribamos

Reflexiones, análisis, analogías, estudios, intereses, acciones, mapas, críticas y ampliaciones ineludibles.

Entintemos la página.

Manuscribamos

Reflexiones, análisis, analogías, estudios, intereses, acciones, mapas, críticas y ampliaciones ineludibles.

Entintemos la página.

Para la composición de la presente edición he utilizado el preparador de documentos LaTeX (Lamport, 1984) —facilitador del uso del sistema de composición tipográfica TeX(Knuth, 1978)—, en su versión LaTeX 2$_\varepsilon$, el sistema de manejo bibliográfico BibTeX (Patashnik y Lamport, 1985), el generador de índices MakeIndex (Chen, 1986) y el compilador LuaLaTeX (Hagen, Henkel, Hoekwater y Scarso, 2007), todos vía la distribución TeXLive (Rahtz, 1996), con la mediación de TeXstudio (van der Zander, Sundermeyer, Braun y Hoffmann, 2009). Para el texto principal he usado Alegreya (Peral, 2010), para los resúmenes, Montserrat (Ulanovsky, Matas, Peral y Le Bailly, rev. 2017), para el lenguaje lógico-matemático, Euler Virtual Math (Euler-VM) (Schmidt, 2002, a partir de las fuentes AMS Euler de Zapf, 1983) y para el código, Source Code Pro (Hunt, 2012, rev. 2019).

Algunas tablas de verdad las ha generado el artefacto *Truth Table Generator* (https://mrieppel.net/prog/truthtable.html) (Rieppel, 2010); a modo de muestra, la del ejemplo 94 (p. 128 de esta edición), a partir de la entrada `((( s > w) &  (s &  c)) & (w > (s & c))) > c` y la del ejemplo 310 (p. 582 de esta edición), a partir de la entrada `((((( p & q) & r) & ( p v q)) & (q v  r)) & (q v  s)) > (p &  q)`. Para las derivaciones formales con recuadros para supuestos que se cancelan he utilizado el paquete *logicproof* (Davidson [228], 2014). Estoy muy agradecido a Peter Smith por su página web *Logic Matters* [229].

En otro orden de cosas, yo, como autor, quisiese quedar exonerado de toda responsabilidad que pudiese derivarse de cualquier circunstancia imputable a terceras personas por el uso incorrecto de lo expuesto en estas notas y que pudiese afectarles de alguna u otra forma.

Sean prudentes y cuídense.

Colofón

I never read. It prevents me from thinking [Nunca leo. Me impide pensar] (Paul Adrien Maurice DIRAC).

¿Se olvida una madre de su criatura,
no se compadece del hijo de sus entrañas?
¡Pero aunque ella se olvide,
yo no te olvidaré!
(Isaías, 49, 15).